AMERICAN BANKRUPTCY INSTITUTE

2017 Northeast Bankruptcy Conference

ESI and Ethics: How to Avoid Sanctions — and Worse

Jonathan Sablone, Moderator
Nixon Peabody LLP; Boston

Charles R. Bennett, Jr.
Murphy & King; Boston

Hon. Hannah L. Blumenstiel
U.S. Bankruptcy Court (N.D. Cal.); San Francisco

John J. Queirolo, Jr.
Innovative Discovery, LLC; New York

Hon. Brian P. Stern
Rhode Island Superior Court; Warwick, R.I.

Amanda Buck Varella
Brown Rudnick LLP; Boston

Fed. Rule Civ. Pro. 37(e)

(e) 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.

I. DUTY TO PRESERVE ELECTRONICALLY-STORED INFORMATION

A. WHEN

1. A duty arises when litigation is pending or reasonably foreseeable. This includes when a party receives a discovery request, a litigation hold notice, or other notification that litigation is likely to be commenced.

2. The 2015 amendments to the FRCP did not alter existing law on the circumstances that trigger the duty to preserve.

3. The Advisory Committee Notes to FRCP 37(e) warn that hindsight may make it seem that it should have been obvious that certain material was relevant when in reality the only alert to the prospect of litigation did not convey the full scope of the relevant material. Courts should try to correct for such hindsight distortion.

B. WHAT

1. A party must take reasonable steps to retain data that could be relevant. The rule does not require "perfection".

2. ESI includes: email, documents in electronic form, voicemails, instant messages, text messages, databases, audio and video recordings, photographs, social media postings and the metadata for all of these.

3. When assessing whether a party's preservation efforts were reasonable, according to the Advisory Committee Notes, a court will consider:

   a) Available resources – a less costly form of preservation is reasonable if it is substantially as effective.

   b) Level of sophistication – preservation efforts are to be judged more leniently where parties, particularly individuals, have no prior familiarity with the obligations.

   c) Level of control over the ESI – to the extent that loss occurs because of third parties, natural disasters or similar, courts will look at whether the party should have known of the risks and protected against them.

   d) Independent requirements for information retention, e.g. statutes, regulations, a party's own policies. (Note however that the Committee explicitly cautions that an independent obligation will not necessary mean that efforts to preserve in the litigation that fall short of this independent obligation are unreasonable for purposes of the litigation.)

e) The routine, good-faith operation of an electronic information system, as under the previous version of the rule, is relevant but only until it is reasonable for the party to intervene in that routine operation.

4. As Preservation Orders become more common, this also becomes the opportunity to specify what preservation steps the parties will take. Courts will expect parties to discuss these questions early and seek resolution regarding disputes early.

5. Examples of actions deemed to be a failure to take reasonable steps:

a) Failure to disable a text message auto-delete function;

b) Failure to preserve ESI, relying instead on a single hard copy that was then lost;

c) Failure to notify email vendor to suspend auto-deletions; and

d) Failure to notify necessary individuals of preservation instructions.

See, e.g., Living Color Enters. v. New Era Aquaculture Ltd., 2016 U.S. Dist. LEXIS 39113, 2016 WL 1105297 (S.D. Fla. 2016) or *Marten Transp., Ltd. v. Plattform Adver., Inc.*, 2016 U.S. Dist. LEXIS 15098 (D. Kan. Feb. 8, 2016).

C. HOW

1. Issue a Litigation Hold Notice to one's own client.

a) Identify topics and types of data and locations of that data.

b) Identify custodians.

c) Identify automatic and manual deletion or destruction systems-organization-wide and on the individual level – that need to stop.

See sample litigation hold letter for own client and litigation hold timeline.

2. Monitor compliance – ask for compliance acknowledgments.

3. Keep compliance records (noting costs and reasons for not taking steps where relevant).

4. Update the litigation hold as the understanding possibly relevant material evolves.

5. Issue a litigation hold notice for opponent.

II. SPOLIATION

The Rule change for ESI was intended to create greater uniformity between jurisdictions.

A. INITIAL REMEDY

1. Court's initial focus will be on whether the lost information can be restored or replaced through additional discovery.

2. Note that there is still a proportionality requirement such that any new discovery needs to be proportional to the apparent importance of the lost information to claims or defenses in the litigation.

B. PROOF REQUIREMENTS

1. If a party can show:

a) (1) the other party had a duty to preserve certain ESI;
b) (2) that party failed to take reasonable steps to preserve that ESI;
c) (3) the ESI was lost because of this failure; and
d) (4) there is no ability to cure a loss of ESI through additional discovery, then Rule 37(e) applies.

See, e.g., *O'Berry v. Turner*, 2016 U.S. Dist. LEXIS 55714 (M.D. Ga. 2016).

2. There are two possible avenues of recourse under Rule 37(e):

a) Subdivision (e)(1) Remedy –Curative Measures: After a finding of prejudice to the moving party, measures that cure but do not exceed the prejudice are authorized. See, e.g., *Simon v. City of New York*, 2017 U.S. Dist. LEXIS 1629 (SDNY Jan. 5, 2017).

(1) The prejudice finding must include an evaluation of the lost information's importance in the litigation.

(2) The rule does not allocate the burden for proving or disproving prejudice to a party, rather it is up to the judge's discretion. It is important to argue the point in any related filings - particularly based on whether the content of the lost information is evident and whether the importance of that information is in debate. (*See* Advisory Committee Notes.)

(3) Possible remedies under provision (e)(1) include:
(a) Forbidding a party to put on certain evidence;
(b) Permitting the parties to present evidence and argument to the jury regarding the loss of ESI;

(c) Giving jury instructions to assist in the evaluation of lost ESI; and

(d) Other additional discovery that has the potential to diminish the harm or clarify what was lost, typically at the expense of the spoliating party. *See, e.g., TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo*, 2017 U.S. Dist. LEXIS 46772 (D.P.R. Mar. 27, 2017).

(4) Curative measures requested under (e)(1) cannot include those permissible only under (e)(2). This especially applies to any application (pre-trial, bench trial, jury instructions, etc.) of the presumption that lost information was unfavorable to the party who lost it.

b) **Subdivision (e)(2) Remedy –Severe Measures:** In the case where there is a finding of an intent to deprive the moving party of the absent information, the court may implement one of the three possible severe measures under the Rule, but does **not** have to use one of these. The court is still obligated to be proportional to the wrong. *See, e.g., DVComm, LLC v. Hotwire Communs., LLC*, 2016 U.S. Dist. LEXIS 13661 (E.D. Pa. Feb. 3, 2016) and *GN Netcom, Inc. v. Plantronics, Inc.*, 2016 U.S. Dist. LEXIS 93299 (D. Del. July 12, 2016).

(1) The three measures are:

(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;

(c) dismiss the action or enter a default judgment.

(2) A negligence finding is not enough for the severe measures. The deprivation of ESI must be intentional.

(3) Examples of findings of intent to deprive include when evidence showed:

(a) Deliberate alteration of relevant documents;

(b) "Double deleting" relevant documents by a tech savy principal;

(c) A supervisor's emailed instructions to delete relevant emails during the course of the matter; and

(d) Deletions of text messages by multiple custodians in the context of other questionable explanations of this behavior.

(4) Some courts are willing to infer intent to deprive simply from a lack of reasonable steps to preserve.

c) Some courts still rely on their inherent authority to impose sanctions so it is still worth arguing in the alternative for remedies under old case law. *See Hsueh v. N.Y. State Dep't of Fin. Servs.*, 15 Civ. 3401 (PAC) (S.D.N.Y. Mar. 31, 2017).

C. OTHER RESOURCES

1. See ABA summary article: https://apps.americanbar.org/litigation/committees/commercial/articles/fall2015-1115-2015-amendment-federal-rule-civil-procedure-37e.html

2. See article by Samantha V. Ettari: http://www.kramerlevin.com/files/Publication/469e2213-d77c-4816-9812-25b6580a0178/Presentation/PublicationAttachment/9d7298a5-8261-4364-8829-119416f97236/Sanctions%20Under%20Amended%20FRCP%2037%28e%29%20One%20Year%20In%20-%20Sam%20Ettari.pdf

3. See Rule 37(e) Notes of the Advisory Committee on the 2015 Amendments. (Attached)

Notes of Advisory Committee on 2015 Amendments. *Subdivision (a).* Rule 37(a)(3)(B)(iv) is amended to reflect the common practice of producing copies of documents or electronically stored information rather than simply permitting inspection. This change brings item (iv) into line with paragraph (B), which provides a motion for an order compelling "production, or inspection."

Subdivision (e). Present Rule 37(e), adopted in 2006, provides: "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system." This limited rule has not adequately addressed the serious problems resulting from the continued exponential growth in the volume of such information. Federal circuits have established significantly different standards for imposing sanctions or curative measures on parties who fail to preserve electronically stored information. These developments have caused litigants to expend excessive effort and money on preservation in order to avoid the risk of severe sanctions if a court finds they did not do enough.

New Rule 37(e) replaces the 2006 rule. It authorizes and specifies measures a court may employ if information that should have been preserved is lost, and specifies the findings necessary to justify these measures. It therefore forecloses reliance on inherent authority or state law to determine when certain measures should be used. The rule does not affect the validity of an independent tort claim for spoliation if state law applies in a case and authorizes the claim.

The new rule applies only to electronically stored information, also the focus of the 2006 rule. It applies only when such information is lost. Because electronically stored information often exists in multiple locations, loss from one source may often be harmless when substitute information can be found elsewhere.

The new rule applies only if the lost information should have been preserved in the anticipation or conduct of litigation and the party failed to take reasonable steps to preserve it. Many court decisions hold that potential litigants have a duty to preserve relevant information when litigation is reasonably foreseeable. Rule 37(e) is based on this common-law duty; it does not attempt to create a new duty to preserve. The rule does not apply when information is lost before a duty to preserve arises.

In applying the rule, a court may need to decide whether and when a duty to preserve arose. Courts should consider the extent to which a party was on notice that litigation was likely and that the information would be relevant. A variety of events may alert a party to the prospect of litigation. Often these events provide only limited information about that prospective litigation, however, so that the scope of information that should be preserved may remain uncertain. It is important not to be blinded to this reality by hindsight arising from familiarity with an action as it is actually filed.

Although the rule focuses on the common-law obligation to preserve in the anticipation or conduct of litigation, courts may sometimes consider whether there was an independent requirement that the lost information be preserved. Such requirements arise from many sources—statutes, administrative regulations, an order in another case, or a party's own

information-retention protocols. The court should be sensitive, however, to the fact that such independent preservation requirements may be addressed to a wide variety of concerns unrelated to the current litigation. The fact that a party had an independent obligation to preserve information does not necessarily mean that it had such a duty with respect to the litigation, and the fact that the party failed to observe some other preservation obligation does not itself prove that its efforts to preserve were not reasonable with respect to a particular case.

The duty to preserve may in some instances be triggered or clarified by a court order in the case. Preservation orders may become more common, in part because Rules 16(b)(3)(B)(iii) and 26(f)(3)(C) are amended to encourage discovery plans and orders that address preservation. Once litigation has commenced, if the parties cannot reach agreement about preservation issues, promptly seeking judicial guidance about the extent of reasonable preservation may be important.

The rule applies only if the information was lost because the party failed to take reasonable steps to preserve the information. Due to the ever-increasing volume of electronically stored information and the multitude of devices that generate such information, perfection in preserving all relevant electronically stored information is often impossible. As under the current rule, the routine, good-faith operation of an electronic information system would be a relevant factor for the court to consider in evaluating whether a party failed to take reasonable steps to preserve lost information, although the prospect of litigation may call for reasonable steps to preserve information by intervening in that routine operation. This rule recognizes that "reasonable steps" to preserve suffice; it does not call for perfection. The court should be sensitive to the party's sophistication with regard to litigation in evaluating preservation efforts; some litigants, particularly individual litigants, may be less familiar with preservation obligations than others who have considerable experience in litigation.

Because the rule calls only for reasonable steps to preserve, it is inapplicable when the loss of information occurs despite the party's reasonable steps to preserve. For example, the information may not be in the party's control. Or information the party has preserved may be destroyed by events outside the party's control—the computer room may be flooded, a "cloud" service may fail, a malign software attack may disrupt a storage system, and so on. Courts may, however, need to assess the extent to which a party knew of and protected against such risks.

Another factor in evaluating the reasonableness of preservation efforts is proportionality. The court should be sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts. A party may act reasonably by choosing a less costly form of information preservation, if it is substantially as effective as more costly forms. It is important that counsel become familiar with their clients' information systems and digital data—including social media—to address these issues. A party urging that preservation requests are disproportionate may need to provide specifics about these matters in order to enable meaningful discussion of the appropriate preservation regime.

When a party fails to take reasonable steps to preserve electronically stored information that should have been preserved in the anticipation or conduct of litigation, and the information is lost

as a result, Rule 37(e) directs that the initial focus should be on whether the lost information can be restored or replaced through additional discovery. Nothing in the rule limits the court's powers under Rules 16 and 26 to authorize additional discovery. Orders under Rule 26(b)(2)(B) regarding discovery from sources that would ordinarily be considered inaccessible or under Rule 26(c)(1)(B) on allocation of expenses may be pertinent to solving such problems. If the information is restored or replaced, no further measures should be taken. At the same time, it is important to emphasize that efforts to restore or replace lost information through discovery should be proportional to the apparent importance of the lost information to claims or defenses in the litigation. For example, substantial measures should not be employed to restore or replace information that is marginally relevant or duplicative.

Note to Subdivision (e)(1). This subdivision applies only if information should have been preserved in the anticipation or conduct of litigation, a party failed to take reasonable steps to preserve the information, information was lost as a result, and the information could not be restored or replaced by additional discovery. In addition, a court may resort to (e)(1) measures only "upon finding prejudice to another party from loss of the information." An evaluation of prejudice from the loss of information necessarily includes an evaluation of the information's importance in the litigation.

The rule does not place a burden of proving or disproving prejudice on one party or the other. Determining the content of lost information may be a difficult task in some cases, and placing the burden of proving prejudice on the party that did not lose the information may be unfair. In other situations, however, the content of the lost information may be fairly evident, the information may appear to be unimportant, or the abundance of preserved information may appear sufficient to meet the needs of all parties. Requiring the party seeking curative measures to prove prejudice may be reasonable in such situations. The rule leaves judges with discretion to determine how best to assess prejudice in particular cases.

Once a finding of prejudice is made, the court is authorized to employ measures "no greater than necessary to cure the prejudice." The range of such measures is quite broad if they are necessary for this purpose. There is no all-purpose hierarchy of the severity of various measures; the severity of given measures must be calibrated in terms of their effect on the particular case. But authority to order measures no greater than necessary to cure prejudice does not require the court to adopt measures to cure every possible prejudicial effect. Much is entrusted to the court's discretion.

In an appropriate case, it may be that serious measures are necessary to cure prejudice found by the court, such as forbidding the party that failed to preserve information from putting on certain evidence, permitting the parties to present evidence and argument to the jury regarding the loss of information, or giving the jury instructions to assist in its evaluation of such evidence or argument, other than instructions to which subdivision (e)(2) applies. Care must be taken, however, to ensure that curative measures under subdivision (e)(1) do not have the effect of measures that are permitted under subdivision (e)(2) only on a finding of intent to deprive another party of the lost information's use in the litigation. An example of an inappropriate (e)(1) measure might be an order striking pleadings related to, or precluding a party from offering any evidence in support of, the central or only claim or defense in the case. On the other hand, it may

be appropriate to exclude a specific item of evidence to offset prejudice caused by failure to preserve other evidence that might contradict the excluded item of evidence.

Subdivision (e)(2). This subdivision authorizes courts to use specified and very severe measures to address or deter failures to preserve electronically stored information, but only on finding that the party that lost the information acted with the intent to deprive another party of the information's use in the litigation. It is designed to provide a uniform standard in federal court for use of these serious measures when addressing failure to preserve electronically stored information. It rejects cases such as *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99 (2d Cir. 2002), that authorize the giving of adverse-inference instructions on a finding of negligence or gross negligence.

Adverse-inference instructions were developed on the premise that a party's intentional loss or destruction of evidence to prevent its use in litigation gives rise to a reasonable inference that the evidence was unfavorable to the party responsible for loss or destruction of the evidence. Negligent or even grossly negligent behavior does not logically support that inference. Information lost through negligence may have been favorable to either party, including the party that lost it, and inferring that it was unfavorable to that party may tip the balance at trial in ways the lost information never would have. The better rule for the negligent or grossly negligent loss of electronically stored information is to preserve a broad range of measures to cure prejudice caused by its loss, but to limit the most severe measures to instances of intentional loss or destruction.

Similar reasons apply to limiting the court's authority to presume or infer that the lost information was unfavorable to the party who lost it when ruling on a pretrial motion or presiding at a bench trial. Subdivision (e)(2) limits the ability of courts to draw adverse inferences based on the loss of information in these circumstances, permitting them only when a court finds that the information was lost with the intent to prevent its use in litigation.

Subdivision (e)(2) applies to jury instructions that permit or require the jury to presume or infer that lost information was unfavorable to the party that lost it. Thus, it covers any instruction that directs or permits the jury to infer from the loss of information that it was in fact unfavorable to the party that lost it. The subdivision does not apply to jury instructions that do not involve such an inference. For example, subdivision (e)(2) would not prohibit a court from allowing the parties to present evidence to the jury concerning the loss and likely relevance of information and instructing the jury that it may consider that evidence, along with all the other evidence in the case, in making its decision. These measures, which would not involve instructing a jury it may draw an adverse inference from loss of information, would be available under subdivision (e)(1) if no greater than necessary to cure prejudice. In addition, subdivision (e)(2) does not limit the discretion of courts to give traditional missing evidence instructions based on a party's failure to present evidence it has in its possession at the time of trial.

Subdivision (e)(2) requires a finding that the party acted with the intent to deprive another party of the information's use in the litigation. This finding may be made by the court when ruling on a pretrial motion, when presiding at a bench trial, or when deciding whether to give an adverse inference instruction at trial. If a court were to conclude that the intent finding should be made by

a jury, the court's instruction should make clear that the jury may infer from the loss of the information that it was unfavorable to the party that lost it only if the jury first finds that the party acted with the intent to deprive another party of the information's use in the litigation. If the jury does not make this finding, it may not infer from the loss that the information was unfavorable to the party that lost it.

Subdivision (e)(2) does not include a requirement that the court find prejudice to the party deprived of the information. This is because the finding of intent required by the subdivision can support not only an inference that the lost information was unfavorable to the party that intentionally destroyed it, but also an inference that the opposing party was prejudiced by the loss of information that would have favored its position. Subdivision (e)(2) does not require any further finding of prejudice.

Courts should exercise caution, however, in using the measures specified in (e)(2). Finding an intent to deprive another party of the lost information's use in the litigation does not require a court to adopt any of the measures listed in subdivision (e)(2). The remedy should fit the wrong, and the severe measures authorized by this subdivision should not be used when the information lost was relatively unimportant or lesser measures such as those specified in subdivision (e)(1) would be sufficient to redress the loss.

USCS Fed Rules Civ Proc R 37

[Corporate Letterhead or Memo from General Counsel]

LITIGATION HOLD NOTICE
(attorney-client communication/attorney work product)

_____ and/or one or more of its subsidiaries (collectively "Company") is either on notice of a probable claim against the Company, or has been named as a party in a pending law suit. Under these circumstances, the Company is obligated to preserve all records, whether hard copy or electronic, that are related to the subject matter of the law suit or claim. Written records include, but are not limited to, word documents, e-mail messages and any attachments, Excel spreadsheets, and Power Point presentations.

SUBJECT MATTER: _____

You have been internally identified as a person who may have records related to the subject matter of the law suit or claim. To protect the Company's rights, you are required to take the following steps:

1.) IMMEDIATELY CONFIRM RECEIPT OF THIS NOTICE:

- Please respond immediately to this message electronically confirming receipt. A copy of this notice and your receipt will be maintained by the Legal Department.
- Include in your response any questions you may have about how to comply with this request.
- When in doubt, preserve records until you have been authorized in writing to do otherwise by the Legal Department.

2.) PRESERVE ALL PAPER WRITTEN RECORDS:

- Identify and maintain in a safe place all hard copy records relating to the subject matter. The documents will be collected by a member of the Legal Department.
- Include all non-identical copies of all documents, including drafts and copies with margin or other notes.
- If you are uncertain whether a document is relevant, err on the side of caution and produce the document.
- DO NOT DESTROY, MUTILATE, OR OTHERWISE MODIFY ANY EXISTING WRITTEN RECORDS.
- A member of the Company's legal staff will contact you for the records.

3.) PRESERVE ALL ELECTRONIC WRITTEN RECORDS:

- Identify all electronic records and their location.
- Electronic records include records in the following locations:
  - Workstation C-Drive
  - Home Computer
  - PDA or Blackberry
  - Memory Sticks/Flash Memory/Thumb Drives

- External Hard Drives
- Back-Up Tapes
- CDs/DVDs

- Maintain all document attachments in their native form. Do not convert existing documents to a different file type.
- **DO NOT OVERWRITE, DELETE OR ALTER ANY EXISTING ELECTRONIC RECORDS, INCLUDING ATTACHMENTS.**
- **IMMEDIATELY CEASE THE USE OF ANY DISK UTILITIES, INCLUDING DEFRAGMENTATION PROGRAMS**
- A member of the Company's IT staff will contact you to arrange a time to copy all electronic records that relate to the subject matter.

If you have any questions regarding this message, please contact the following Legal Department representative immediately.

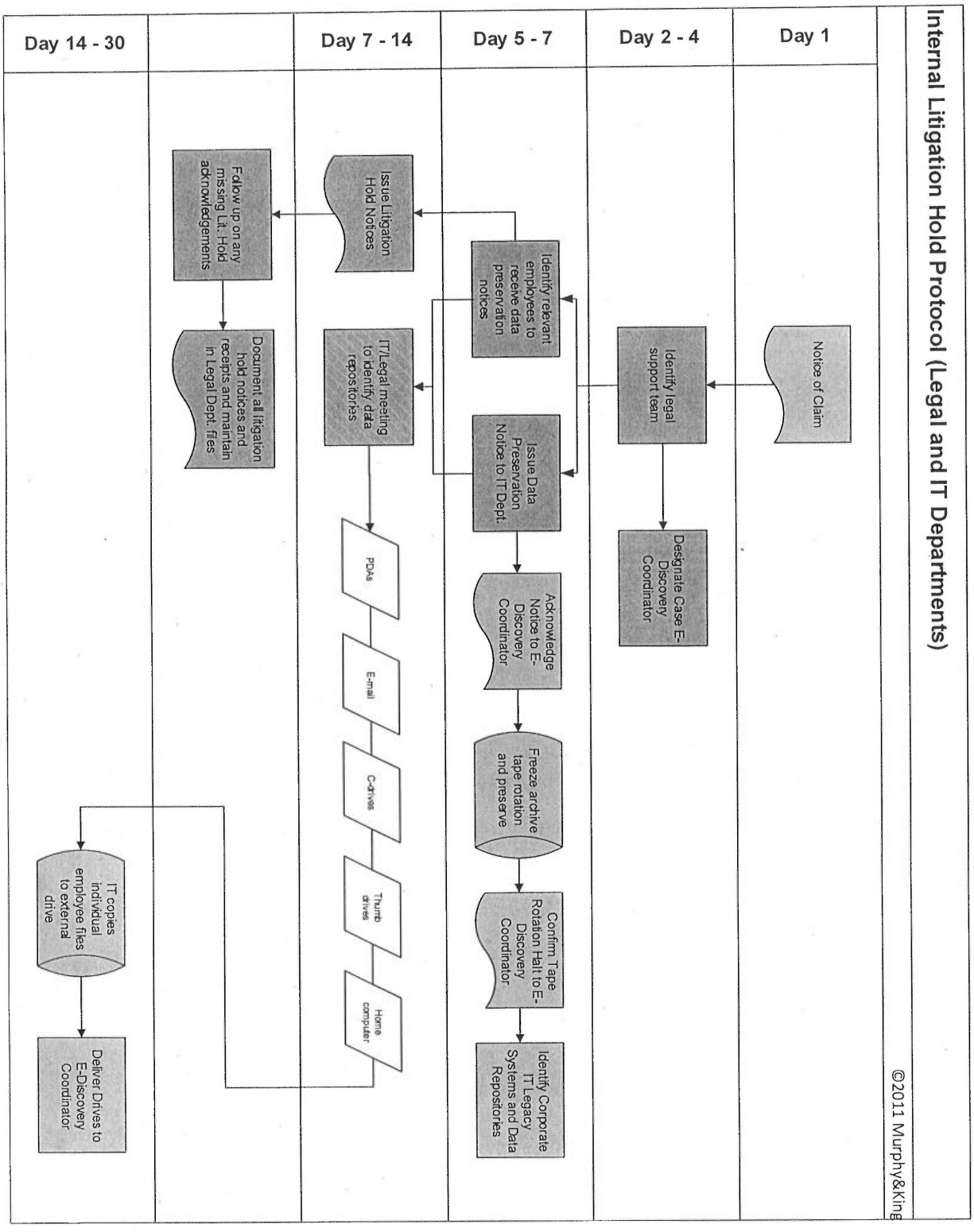
Name:
Telephone:
E-Mail:

If you are not contacted by a member of the IT Department within____days, you should contact your Legal Department representative immediately.

FAILURE TO STRICTLY ADHERE TO THE ABOVE INSTRUCTIONS COULD RESULT IN EXTREME PENALTIES AGAINST THE COMPANY, AND WILL SUBJECT YOU TO IMMEDIATE DISCIPLINARY ACTION, INCLUDING POSSIBLE TERMINATION OF EMPLOYMENT FOR CAUSE.

This notice concerning a potential or actual law suit against the Company is a CONFIDENTIAL PRIVILEGED COMMUNICATION. You are not to disclose or discuss the contents of this notice to anyone other than the Legal and IT staff members who contact you.

588143


Internal Litigation Hold Protocol (Legal and IT Departments)
©2011 Murphy&King
Day 1
Day 2 - 4
Day 5 - 7
Day 7 - 14
Day 14 - 30
Notice of Claim
Identify legal support team
Designate Case E-Discovery Coordinator
Identify relevant employees to receive data preservation notices
Issue Data Preservation Notice to IT Dept.
Acknowledge Notice to E-Discovery Coordinator
Freeze archive tape rotation and preserve
Confirm Tape Rotation Halt to E-Discovery Coordinator
Identify Corporate IT Legacy Systems and Data Repositories
Issue Litigation Hold Notices
IT/Legal meeting to identify data repositories
PDAs
E-mail
C-drives
Thumb drives
Home computer
Follow up on any missing Lit. Hold acknowledgements
Document all litigation hold notices and receipts and maintain in Legal Dept. files
IT copies individual employee files to external drive
Deliver Drives to E-Discovery Coordinator

REPRINT

CD corporate disputes

BRING YOUR OWN DILEMMAS – 'CUSTODY' IN THE DIGITAL AGE

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
APR-JUN 2017 ISSUE

www.corporatedisputesmagazine.com

Visit the website to request
a free copy of the full e-magazine

NIXON PEABODY

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

www.corporatedisputesmagazine.com

PERSPECTIVES

BRING YOUR OWN DILEMMAS – 'CUSTODY' IN THE DIGITAL AGE

BY **JONATHAN SABLONE AND RONALDO RAUSEO-RICUPERO**
> NIXON PEABODY LLP

In today's litigation landscape, digital evidence resides on a wide array of platforms across multiple custodians. With many companies substantially expanding their bring your own device (BYOD) policies, whereby an employee owns the device upon which company data is accessed or stored, it is more crucial than ever for businesses to have a clear understanding of who – the employer, the employee or some other third party – maintains legal possession, custody or control over their sensitive business information when it resides on a device that is also intended for the employee's own personal use. These policies can have serious implications for the ability to secure evidence that may be crucial to the prosecution or defence of a case.

Under the Federal Rules of Civil Procedure, parties to a litigation and non-parties who are subject to deposition or written subpoena are required to produce electronically stored information (ESI) within that entity's "possession, custody or control," yet the Rules do not define any of those three terms and courts are then left to consider their meaning in particular circumstances, often with divergent results. The interpretations vary so widely that some federal courts will preface their rulings in this area with warnings that "the federal courts are divided on

when and how a party seeking discovery can access ESI stored on an employee's personal device".

Putting BYOD policies to the test

Last August, in the face of this broad range of interpretive standards articulated by courts across the country, the Sedona Conference, a leading e-discovery think tank, joined in the debate with a substantial report on "possession, custody or control", identifying three main trends in these opinions which can help guide the analysis for companies with BYOD.

The most common approach, the 'Legal Right Test', used in eight judicial circuits, will result in a court ordering production of ESI where the party has the "legal right" to obtain the documents, such as through direct custody, through an agreement with a service provider granting them the automatic right to obtain the information, or through a parent company's legal control over its subsidiaries (e.g., *Cotton v. Costco Wholesale Corp.,* 2013). The Legal Right Test will apply most squarely to those companies with written BYOD policies whereby employees explicitly provide advance consent that

all company-generated content on their devices is legally owned by the company. Many such consent agreements will allow the employer express rights to monitor the personal device, to install the company's own software on the device, to copy the data on the devices specifically for the purpose of complying with legal retention, and to access the device remotely and remove company information at the conclusion of the individual's term of employment. Practically, many companies will use the device's own mobile device management (MDM) features to perform remote configuration, or will establish a password-restricted 'sandbox' within the device's virtual architecture.

For courts using the 'Legal Right Test', attempts to reach into an employee's personal accounts in the absence of prior consent by employees will not likely succeed. In *Matthew Enterprise v. Chrysler Group*, 2015, although many of the defendant's employees were not issued email addresses on the defendant's email system and therefore used their own personal email accounts for work purposes, the court ruled that the defendant could not be ordered to collect emails from employees' personal accounts because they did not have legal control over those accounts. It further found that an employee handbook instructing employees to keep corporate information in the "sole possession" of the employer was not sufficient to demonstrate that legal control over personal emails had been granted by the employees to the employer.

In four judicial circuits, the courts will apply the 'Legal Right Plus Notification Test', which requires the responding party both to produce materials within its legal control and also to identify custodians outside its legal control who may possess responsive information, presumably so that the requesting party can evaluate whether to seek the materials from those non-party custodians through its own discovery efforts. This standard would have the greatest impact on those businesses with employees who are using their own personal accounts, such as personal email addresses, personal mobile smartphone texting accounts, or personal social media accounts to conduct activities related to the subject matter of the lawsuit.

Finally, the courts in six judicial circuits apply some version of the 'Practical Ability Test' pursuant to which a party will be obligated to produce not only the material in their legal control, but also ESI that they have the 'practical ability' to obtain from a non-party to the action. Some courts have found this test to require producing parties to actively request information from non-parties in order to satisfy their own discovery obligations, a departure from general discovery principles (e.g., *Anz Advanced Techs. v. Bush Hog, LLC*, 2011). This final test could pose the most substantial complications for BYOD practices that involve employees' personally-owned accounts, because it can be read to obligate, for example, an employer defendant to ask employees to produce

materials that the employers themselves could not otherwise legally access.

Aggressive use of this test can also result in onerous obligations on parties; for example, in *Export-Import Bank of the United States v. Asia Pulp & Paper Co.*, a plaintiff was forced to ask its former employees to cooperate in a collection before the plaintiff could assert that it had no control over documents in the former employees' possession. In 'Practical Ability Test' jurisdictions, preservation obligations will extend to personal devices which a defendant has 'practical ability' to control. *Living Color Enterprises, Inc. v New Era Aquaculture Ltd.*, 2016, found that the defendant had a duty to preserve text messages maintained on his personal phone and that destruction of the texts and failure to disable the auto-delete function could constitute intentional destruction of relevant ESI. Failure to preserve information on personal devices in accordance with legal requirements can, in turn, result in spoliation. *Brown Jordan Int'l, Inc. v Carmicle*, 2016, found adverse inference sanction justified as a result of spoliation of metadata on a 'bring your own device', when the defendant failed to preserve ESI from "his personal iPad, his personal laptop computer, the company-owned laptop, the company-owned iPad, [his] personal iPhone and [his wife]'s computer".

The Sedona Conference criticises the Practical Ability Test on several bases. These include contentions that it complicates contractual agreements under which, for example, a non-disclosure or confidentiality agreement would be breached by producing information to a requesting party in discovery, it disregards the corporate form and does not sufficiently account for the often more-stringent privacy laws at issue in foreign jurisdictions.

"In 'Practical Ability Test' jurisdictions, preservation obligations will extend to personal devices which a defendant has 'practical ability' to control."

Most relevant to BYOD is the concern that this test could spur requests for employee data that could run counter to the Stored Communications Act (SCA) which prohibits employers from accessing their employees' personal online information in an unauthorised manner. *Pietrylo v. Hillstone Restaurant Group*, 2009, held that an employer requesting the password of an employee was coercive and in violation of the SCA because the employee believed that she "would have gotten in trouble" if

she refused to provide the login credentials. More than a dozen states have enacted specific statutes prohibiting employers from seeking employees' password information. Moreover, even if an employer does gain access to the personal device, there may still be potential liability if the employer accesses health-related information during the collection.

Bring your own diligence

Given these circumstances, companies should be mindful of the applicable test, or variation thereof, at issue in their particular jurisdiction and weigh the implications of obtaining advance written consent of employees in a BYOD policy. In some cases they may choose to forgo written policies so as to not add contractual obligations beyond what the case law would require. While some companies may also consider obtaining prior consent from employees for access to work-related information held in employees' personal accounts for litigation purposes, businesses should carefully consider both whether that step would comply with applicable statutory obligations, and whether they are truly prepared to undertake the attendant retention, preservation, collection and production obligations over material that would then be within their control, but largely out of their hands. CD

Jonathan Sablone
Partner
Nixon Peabody LLP
T: +1 (212) 224 6395
E: jsablone@nixonpeabody.com

Ronaldo Rauseo-Ricupero
Associate
Nixon Peabody LLP
T: +1 (617) 345 1071
E: rrauseoricupero@nixonpeabody.com