A Primer on Document Retention and Disclosure Requirements for In-House Counsel

By William D. Furnish

Osborn Maledon, P.A.

I. Introduction

Few people start a business or enter legal practice to become experts in data storage. In the event of litigation, however, companies look to in-house counsel and their IT departments to quickly assess the merits of a potential dispute and meet discovery obligations. Although the issues are mundane, waiting until a demand letter or complaint is served to understand how your company uses, stores, and preserves electronic and hard copy files will often result in the loss of information that is critical to the merits of a legal dispute and complying with disclosure requirements under State and Federal law. Failing to meet these disclosure requirements, inadvertent or otherwise, reduces the chance of victory on the merits and may result in serious court sanctions. With these risks in mind, this article provides a high-level overview of document management and retention prior to and during litigation.

II. Normal Company Operations—Before Litigation

Company leadership, in-house counsel, and IT department staff should have a coordinated understanding of how a company generates documents (particularly electronic data), where the company stores those documents, and how long they are retained. Having a firm grasp on this information, along with a developed, enforced document retention policy, allows a company to save money in storage costs, eliminate stale data, and transition seamlessly to litigation discovery in the event it needs to quickly locate, preserve, review and disclose documents.

a. Understanding the Information Landscape

Rightly, business goals and efficiency drive the generation and retention of information. In-house counsel should understand:

- Whether the company has in-house or outsourced IT;
- The primary point of contact in IT and records for electronic and physical document recovery;
- What types of programs different company units use and what types of file formats these programs create;
- What forms of internal communication the company uses and which of those forms are stored electronically—email, instant messenger, electronic file transfers, digital voicemail, text messages, and other electronic formats; and
- How often, for how long, and where electronic data is backed up.

Understanding will allow in-house counsel to cause fewer disruptions to business units and explain internal practices to outside counsel, opposing parties, and the court. It will also help counsel understand how many resources it will have at its disposal in the event of a legal dispute.

b. Structuring the Information Landscape

In-house counsel should be familiar with a company's document retention policy (or put one in place) and should work with the company's IT department to ensure it is up-to-date based on the company' practices and its legal obligations. The following are considerations relevant to those policies.

Length of Preservation: Aside from industry-specific regulations mentioned below, there is no general requirement that documents be preserved indefinitely, or even for a specific period of time. Business units, in-house counsel and IT should consider the needs of the company and the costs of storage of electronic and hard copy data when determining where and for how long information is retained. Setting and adhering to a retention period for data has the advantage of lowering storage costs, reducing the amount of data to be collected and searched in the event of litigation, and eliminating stale data that could make mischief in later litigation when taken out of context. Moreover, in the event of destruction prior to the anticipation of a legal dispute, a clear document retention policy will demonstrate to a court or government investigator that the destruction was justified and not undertaken to conceal harmful information.

Industry-Specific Requirements: Specific industries, such as medicine and financial services, will often have government-mandated data security and preservation requirements with which in-house counsel must ensure compliance. For instance, Arizona—among other jurisdictions—imposes specific requirements on the retention of medical records by health care providers,[1] and HIPAA imposes further requirements on the security and storage of that information.[2] Similarly, the Securities and Exchange Act requires regulated companies to retain email for at least three years.[3] Military contractors may be required to store data on secure servers maintained by the government. Retention policies should also take into consideration whether the company has agreements with clients or other third-parties governing how long and in what form documents are retained.

[1] A.R.S. § 12-2297.

[2] 45 C.F.R. § 164.530(c).

[3] Securities and Exchange Act, Rule 17a-4, 17 C.F.R. § 240.17a-4.

Other Document Retention Policy Considerations: The document retention policy should outline appropriate use of company technology, and provide guidelines on how documents are to be organized, stored, and retained.[4] The policy should specifically detail how litigation holds are initiated and enforced, as well as identifying: (1) what individual and department is responsible for enforcing and updating the policy; (2) whether documents are retained after individuals are terminated or leave the company; (3) whether and how documents should be stored on local hard drives or on network folders; and (4) whether email and other data is migrated in the event of a change in servers.

Although in-house counsel and company units will naturally focus on how email and electronic files like word documents, spreadsheets and PDF files are preserved, they should also be cognizant of the company's policies regarding the storage of instant messaging, SMS, voicemail, and text messages. The document retention policy should clearly communicate to employees that these media, along with work-issued smartphones and PDAs contain company information that may subsequently be discoverable in a lawsuit or government investigation. In one somewhat recent example, numerous recorded Bloomberg Messenger conversations revealed a large LIBOR-rigging effort by several large banks that continues to generate litigation.[5]

III. Litigation "On the Horizon"[6]

As discussed above, there is no general requirement to preserve documents in a company setting indefinitely. Information that is relevant to a potential legal dispute must be preserved, however, when a lawsuit or investigation is "reasonably anticipated."[7] Although the concept of

---

[4] For a further discussion on the cyber security components of a document retention policy, *see* Danielle Janitch and John Blanchard's comprehensive chapter in this publication entitled "Building a CyberSecurity Resource Toolbox for Your In-House Legal Department," as well as Ms. Janitch's collected publications on these issues available at http://www.omlaw.com/attorneys/bio/danielle-d-janitch/.

[5] *See* Tom Braithwaite, "Banks to Gain More Control over Trader Chat via Bloomberg," Financial Times (12/17/13) *available at* https://www.ft.com/content/7d260c48-6720-11e3-a5f9-00144feabdc0.

[6] For a more in-depth discussion of litigation holds and the potential harm from failure to implement those holds that informs this section, *see* Nicholas J. Panarella, "Implementing a Litigation Hold," Westlaw Practical Law Practice Note 8-502-8481 (2017) and The Sedona Conference, "Commentary on Legal Holds: The Trigger & The Process," 11 Sedona Conf. J. 265 (2010).

[7] Ariz. R. Civ. P. 37(g) ("A party or person has a duty to take reasonable steps to preserve electronically stored information relevant to an action once it commences the action, once it learns that it is a party to the action, or once it reasonably anticipates the action's

reasonably anticipated litigation is nebulous, courts may determine that a company should have reasonably anticipated litigation when the company:

- Anticipates initiating a lawsuit against a third-party;
- Receives a demand letter or notice of claim from a potentially adverse party or a credible verbal threat of litigation;
- Receives a whistle-blower letter from an employee;
- Files an incident report related to an on-the-job accident;
- Receives a third-party subpoena in an existing lawsuit; or
- Is notified of the commencement of an investigation against it by a federal, state, or other regulatory entities.

a. Instituting a Litigation Hold

Once a company reasonably anticipates litigation—either that it will commence litigation, be served with a lawsuit, or be investigated—it should immediately issue a "litigation hold letter" to employees involved in the relevant dispute and its IT department to suspend the destruction of documents that may be relevant in the potential dispute. The company should then take steps to document that the litigation hold is actually enforced. This step is of critical importance because—in the event of unintentional destruction of relevant, discoverable information—a company may avoid or mitigate sanctions by demonstrating that it took "reasonable steps" to preserve information.

A litigation hold letter need not spell out all details of the potential dispute—particularly to avoid alarming employees or creating the impression of wrongdoing by the company where none has occurred. Nevertheless, the litigation hold letter should explain the nature of the potential dispute and the parties involved. The letter should identify the types of documents likely to be requested by the adverse party, the format of those documents, and where they are located. The letter should also identify the individuals responsible for enforcing the hold in the IT department and in-house counsel. For reference, a template litigation hold letter is enclosed as **Appendix 1**.

As part of a litigation hold, counsel working with the company's IT department should conduct fact gathering interviews of the employees most familiar with the dispute to learn what documents were created, where they are stored, and who else may have information about the dispute. As new facts are learned—either through internal investigation or over the course of the lawsuit—new custodians and categories of documents should be included in the litigation hold.

---

commencement, whichever occurs first."); Fed. R. Civ. P. 37(e) (permitting the imposition of sanctions "if electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost").

b. Sanctions For Document Destruction

The destruction of evidence, frequently referred to as "spoliation," has serious consequences. A company's failure to take reasonable steps to preserve relevant documents in litigation can result in sanctions for spoliation of evidence, either under specific rules of civil procedure or the court's inherent sanction power.[8] Sanctions can range from whatever action a court deems necessary to cure the prejudice caused by the failure to preserve documentation to, in the case of intentional destruction, dismissal of the action or entry of a default judgment.[9]

Sanctions rules, however, are not rules of strict liability. A company may demonstrate that it took reasonable steps to avoid destruction, and thereby avoid or minimize sanctions, with a clearly-defined and enforced document management policy, institution of a litigation hold, and the speedy collection of potentially relevant information.[10] A company that has destroyed information it had a duty to preserve may also defeat sanctions by showing that there was no prejudice caused by the destruction of the documents,[11] although this is often a difficult path given that the information no longer exists.

IV. Litigation – Disclosure and Discovery

Having and enforcing a document preservation policy, coordinating with and understanding IT, and properly instituting a litigation hold give in-house counsel and the company firm footing to commence litigation. At this stage, in-house counsel will, if possible, have turned the day-to-day operations of the matter over to outside counsel with expertise in civil procedure and discovery matters. However, there are a handful of litigation matters of which in-house counsel should be mindful.

a. Disclosure and Discovery Planning

Discovery rules vary from jurisdiction to jurisdiction, particularly with respect to disclosure and document discovery planning requirements. Unlike most jurisdictions, Arizona has affirmative and continuing disclosure requirements under which parties to litigation must

---

[8] Ariz. R. Civ. P. 11, 26(f) & 37(g)(2); Fed. R. Civ. P. 11, 26(f) & 37(e).

[9] Ariz. R. Civ. P. 37(g)(2)(B); Fed. R. Civ. P. 37(e)(2).

[10] Arizona Rule of Civil Procedure 37(g)(1)(C) provides an extensive list of factors for a court to consider in determining whether reasonable steps were taken to prevent the destruction of documents, including whether "the information was lost as a result of the good-faith routine operation of an electronic information system" and the "timeliness of the party's actions."

[11] *See* Ariz. R. Civ. P. 37(g)(2)(A); Fed. R. Civ. P. 37(e)(1).

divulge information on their own initiative to the opposing party.[12] Most other states and the federal court system (subject to the adoption of a pilot program currently being tested) do not have such proactive disclosure requirements.[13]

Arizona and federal rules also diverge regarding the need for a discovery plan. Federal rules require the parties attempt to negotiate in good faith on discovery issues, including the creation of a discovery plan covering the subjects on which discovery will be needed and the format for discovery.[14] Arizona law currently has similar requirements for cases referred to the Complex Civil Litigation Program,[15] with numerous changes to discovery rules—including a tiered system based on matter size and complexity—to come into effect on January 1, 2018.[16]

b. Discovery As a Third-Party to Litigation

Even when a company is not a party to a lawsuit, its participation may be compelled through the receipt of a subpoena.[17] Upon the receipt of a third-party subpoena, a company should issue a litigation hold to ensure it does not destroy potentially responsive information. A company's obligations in responding to a third party subpoena are necessarily less onerous than those of a party,[18] and the scope of such subpoenas often may be narrowed through collaboration with issuing counsel.

---

[12] *See* Ariz. R. Civ. P. 26.1(b) (requiring affirmative disclosure of hard copy documents and electronically stored information).

[13] *See, e.g.*, Fed. R. Civ. P. 26(a)(1)-(3). The United States District Court for the District of Arizona is currently piloting a program requiring mandatory initial discovery responses similar to those required under Arizona's rules for most cases commenced on or after May 1, 2017. *See In re Mandatory Initial Discovery Pilot Project in the District of Arizona*, General Order 17-08 (D. Ariz. Apr. 14, 2017), *available at* http://www.azd.uscourts.gov/sites/default/files/general-orders/17-08.pdf.

[14] Fed. R. Civ. P. 26(f)(3).

[15] Ariz. R. Civ. P. 16.3.

[16] *See In re Various Arizona rules of Civi*l Procedure, No. R-17-0010, Order Amending the Arizona Rules of Civil Procedure and Related Provisions (Ariz. Aug. 31, 2017), *available at http://www.azcourts.gov/Portals/20/2017%20Rules/17-0010.pdf*.

[17] Ariz. R. Civ. P. 34(c), 45; Fed. R. Civ. P. 34(c), 45.

[18] *See* Ariz. R. Civ. P. 34(e)(1) ("A party or attorney responsible for serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena . . . . The issuing court . . . may impose an appropriate sanction—on any party or attorney who fails to comply."); Fed. R. Civ. P. 34(d) (same).

c. Protective Orders and Confidentiality

Companies often have serious concerns about the production of documents as it pertains to the disclosure of confidential and proprietary company information and other potentially sensitive information. A well-crafted protective order ensures that such sensitive information is not disclosed to the public and, in the case of particularly sensitive information, visible only to an adversary's attorney.[19]

There are several caveats to keep in mind regarding protective orders. A company's designation of materials as confidential or attorney's eyes only may be challenged, and courts may reject applications to file such materials under seal. In the event that such designations are accepted, in-house counsel should try to balance preserving confidential information with the inconvenience and delay of managing the filing of matters under seal.

Such designations are particularly important because documents in a company's possession and potentially relevant to the litigation may also be subject to confidentiality agreements or other similar arrangements with third parties.[20] A best practice under these circumstances is to coordinate with the third-party to ensure that they do not object to the disclosure of any documents subject to confidentiality agreements, or would agree to that disclosure as confidential or attorney's eyes only under the Protective Order.

d. Legal Privilege[21]

In-house counsel, at the very least, should have an understanding of the different forms of legal privilege, some of which, like the attorney-client privilege, require attorney involvement and the provision of legal advice, while other legal privileges, like the work product doctrine, do not.[22] Additionally, different privileges are more resilient to waiver: the attorney-client privilege requires confidentiality and can be waived against all parties through disclosure,

---

[19] *See* Ariz. R. Civ. P. 26(c); Fed. R. Civ. P. 26(c).

[20] This area is particularly fraught in cross-border discovery issues where there are greater protections on the disclosure of private materials than in the United States. *See* The Sedona Conference, "Practical In-House Approaches for Cross-Border Discovery and Data Protection," 17 Sedona Conf. J. 399 (2016).

[21] Legal privilege is addressed only briefly here because Jeffrey Molinar has covered this issue in-depth in his chapter of this guide entitled "Protections & Pitfalls of the Attorney Client Privilege."

[22] *See* Ariz. R. Evid. 502 (discussing attorney client privilege and work product protection); Fed. R. Evid. 502 (same); Ariz. R. Civ. P. 26(b) (work product doctrine); Fed. R. Civ. P. 26(b) (same).

whereas the work product doctrine is heartier and can be partially waived while preserving the privilege for other materials.[23]

V. Conclusion

Disclosure and discovery in litigation presents many dangers for companies and in-house counsel that have not developed clear, enforced document retention policies and do not have a clear understanding of their electronic and hard-copy document environment. These dangers include waste of resources, monetary sanctions, and potentially unfavorable judgments. Fortunately, as discussed above, many of these dangers can be easily avoided with foresight and coordination with the company's IT department.

[23] *See* 1 Ariz. Prac., Law of Evidence § 501:5 (4th ed.) (providing a survey of the law regarding attorney-client privilege); *id.* § 501:6 (same for work product doctrine).

APPENDIX 1 – LITIGATION HOLD LETTER TEMPLATE

PRIVILEGED & CONFIDENTIAL
PROTECTED BY THE ATTORNEY-CLIENT PRIVILEGE
AND/OR THE WORK PRODUCT DOCTRINE

To: [Name of business unit or simply "Distribution"]

cc: [IT Department Individuals / Other Members of General Counsel's office involved in managing litigation hold]

From: [General Counsel / primary attorney responsible for litigation hold]
[Title]
[Company Name]

Date:

Re: Litigation Hold Directive to Preserve Data & Documents Related to [Adverse Party]

[Brief description of the active, potential dispute, government investigation or third-party subpoena triggering the litigation hold. Confine the issue to dry facts and do not be alarmist or blasé in your language in describing the matter to employees.]

The purpose of this memorandum is to notify you of the [potential lawsuit / government investigation / subpoena] and to instruct you to ***take all steps necessary to preserve and retain all documents and data***—whether written or electronic—that may be relevant to the product and issues in the Dispute. This includes documents and data that exist today ***and any new documents and data that are created in the future***. In particular, retain all documents and data related to the following:

- [Describe the types and categories of documents that could be relevant to the matter in a detailed manner—e.g., "Documents and data related to incident report number #" or "Documents and data related to contract negotiations between Company and Potential Adversary for contract X."]

IMMEDIATELY STOP destruction, alteration, discarding or deletion of any relevant documents, whether done according to existing record retention schedules or otherwise. You must immediately collect and move all potentially relevant e-mails from your inbox and sent-mail box to a personal folder so that they are not inadvertently or automatically deleted. [Suggest a title for the email folder.] Likewise, move other relevant electronic files on your computer(s) to a folder on your computer also titled [Folder name] and move all paper documents to file folders in a secure place in your office. If there is relevant data on a shared drive, please contact [IT Department / General Counsel's Office employee responsible for managing litigation hold]. ***You must also preserve relevant documents created in the future***.

The failure to preserve and retain the electronic data outlined in this memo could result in negative consequences to [Company Name], including court-ordered penalties and sanctions.

APPENDIX 1 – LITIGATION HOLD LETTER TEMPLATE

The format of potentially relevant documents includes: [**DELETE AS APPROPRIATE BASED ON THE TYPES OF PROGRAMS USED BY THE COMPANY AND RELEVANT TO THE LITIGATION HOLD**]

- e-mail (sent and received, whether internally or externally together with any attachments),
- instant message conversation history(folder in Outlook),
- letters, memos, or other types of correspondence, including electronic files created in Microsoft Word or another word processing programs,
- Excel or other types of spreadsheets, databases,
- presentation slides or scripts, including electronic files created in PowerPoint or other software,
- drafts of documents, presentations, etc.,
- diagrams, drawings, photos and videos,
- handwritten notes,
- voice mail recording,
- business diaries or calendars,
- data generated by calendaring, task management, and personal information management (PIM) software (such as Microsoft Outlook or Lotus Notes), and
- data created with the use of personal data assistants (PDA's), such as [List device types provided to employees], or other mobile devices.

Such data may be located in any of the following locations: networks, workstations, laptops, personal computers, personal e-mail accounts used for work functions, personal data assistants, voicemail, instant messages, CDs, discs, flash drives, USB drives, digital cameras, backup tapes, or history and usage logs.

If you are uncertain whether to keep or destroy any documents, keep them. As stated above, it is imperative that you do not destroy, alter, discard or delete any documents that are even potentially relevant to any of the issues in the anticipated arbitration. That obligation to preserve includes all documents stored in long-term retention, as well as documents in your office or in central files.

If you are aware of other individuals who are not listed on the distribution for this memo but who may have documents or materials relating to its subject matter, please advise [IT Department / General Counsel's Office employee responsible for managing litigation hold]. You may be contacted by a member of the [Company's] legal team to discuss and collect relevant data. In the interim, do not discuss the [potential litigation / government investigation / third-party subpoena] with [Company] employees other than those in the legal department or IT department.

Thank you for your cooperation and do not hesitate to contact me with any questions.