Cloud Computing and Social Media: Electronic Discovery Consideration and Best Practices:

Ashish Prasad
Discovery Services, LLC
Chicago, IL

Elizabeth
Reed Smith
Philadelphia, PA

Steven Puiszis
Hinshaw & Culbertson
Chicago, IL

I. INTRODUCTION

Social media platforms, which include applications such as Facebook, Twitter, and LinkedIn, are immensely popular. According to one source, seventy-five percent of people aged 18 to 24 have profiles on social networking sites like Facebook, while one-third of people aged 35 to 44, and nearly twenty percent of people aged 45 to 54, have profiles on social networking sites. These sites have millions of users, with Facebook alone reporting over eight hundred million users worldwide.

---

1 Jay E. Grenig, Jeffrey S. Kinsler & Lucia Nale, Social Media, 10 ILL. PRAC., CIVIL DISCOVERY § 23:75 (2011).
Applications like Facebook, Twitter, and LinkedIn are merely examples of a proliferating universe of online social networks. These networks share a number of common features. Social networking sites are “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.”

---

I. INTRODUCTION

Social media platforms, which include applications such as Facebook, Twitter, and LinkedIn, are immensely popular. According to one source, seventy-five percent of people aged 18 to 24 have profiles on social networking sites like Facebook, while one-third of people aged 35 to 44, and nearly twenty percent of people aged 45 to 54, have profiles on social networking sites. These sites have millions of users, with Facebook alone reporting over eight hundred million users worldwide. Applications like Facebook, Twitter, and LinkedIn are merely examples of a proliferating universe of online social networks. These networks share a number of common features. Social networking sites are “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.”

---

Further, social media are just a subset of a larger category of applications generally referred to as cloud computing. Cloud computing encompasses various platforms that users can access over the Internet, in which the storage of data is diffused across a potentially large number of sites. Examples of cloud computing include many free web-based applications such as email accounts and document sharing provided by Google, as well as more complex cloud computing systems that are used by companies who are looking to reduce IT management and maintenance costs by using third-party service providers.

Social media and cloud computing are increasingly becoming fixtures of the daily life of companies and their employees. Companies increasingly utilize social networking sites to advertise, communicate with the public, and recruit new employees. Furthermore, other users may create profiles or pages for a company without that company’s knowledge or control. Even if companies themselves are not utilizing social networking sites, many employees are accessing these sites at work for personal purposes.

This widespread and often uncoordinated use of social media means that employers risk being exposed to liability as a result of their own or their employees’ online conduct regarding social media sites. By sending messages through social networking sites, employees may potentially misappropriate intellectual property or other confidential information. In addition, employees may

---

5 *Id.*
7 *Id.* at 488.
8 *Id.* at 491.
distribute materials, photographs or messages through these sites that could expose their employers to harassment or other charges.\textsuperscript{9} Courts could interpret an employee’s use of a workplace computer for personal purposes, including the use of social networking sites, as being within the scope of employment in certain circumstances. Liability could arise when, for example, “such use is reasonably expected in the modern workplace, and the possibility exists that the employer maintains control over use of the computer.”\textsuperscript{10}

More generally, social media may be the subject of discovery, and the need to respond to discovery of social media content in a cost-effective and legally defensible way is a growing concern for businesses. A recent survey conducted by Deloitte Forensic Center found that two-thirds of businesses worry about electronic discovery risks pertaining to social networks, and a majority of companies (58 percent) are not fully prepared to deal with those risks.\textsuperscript{11} Furthermore, in many companies, executives lacked appropriate knowledge or awareness of the challenges of meeting electronic discovery requirements.\textsuperscript{12}

The remainder of this paper is organized as follows. Part II provides an overview of the discoverability of data in the cloud, with particular attention to social media. Data stored in the cloud will often be judged within the “possession, custody, or control” of a litigant and therefore potentially discoverable. However, considerations of relevance, undue burden, and privacy are relevant in determining whether courts will compel production of data in the cloud. Part III then turns to potential strategies and best practices for working with third-party providers of cloud data storage. It is essential to anticipate the potential demands of the discovery process

\textsuperscript{9} Id.
\textsuperscript{10} Id. at 492 (discussing \textit{Booker v. GTE.net LLC}, 350 F.3d 515, 516-17 (6th Cir. 2003)).
\textsuperscript{11} Social Networks Pose E-Discovery Risks, TECHWEB, June 17, 2010, \textit{available at} 2010 WLNR 12370605.
\textsuperscript{12} Id.
when choosing and contracting with a provider. Part IV then adds a discussion of strategies and best practices when dealing with the possibility of social media information that is not directly controlled by a company, but accessed or created by its employees. Part V provides some concluding remarks about the future of cloud-based discovery.

II. WHEN DATA IN THE CLOUD COULD BE SUBJECT TO DISCOVERY

The Federal Rules of Civil Procedure recognize the essential place of electronic documents in the discovery phase of litigation. Courts may consider information stored on the cloud, including private social networking information, to be discoverable. The Federal Rules require initial disclosure to opposing parties of the location of information to be used in support of defenses or claims, under FRCP 26(a)(1)(A)(iii). This could include information in the cloud. Under Rule 45 of the Federal Rules of Civil Procedure, third parties, including government agencies, may issue subpoenas for relevant data directly to the cloud provider, without providing notice to the litigant. In such cases, a litigant may not even know what data is being produced, let alone be able to review that data for privilege or trade secrets before its production.

The production of electronic records pertaining to social media is relatively new in the realm of electronic discovery. The existing framework of rules and practices relating to e-discovery do not adequately encompass discovery pertaining to social

---

14 For a specific example, see Order Regarding Plaintiffs' Motion for Protective Order Pursuant to Fed. R. Civ. P. 26(c) Regarding Subpoenas Issued to Facebook, MySpace, Inc., and Meetup.com, Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009) (ruling that private social networking information is discoverable when the information is relevant).
16 FED. R. CIV. P. 45.
networking sites, as the technology has been outpacing the revision of existing rules and regulations. Courts have indicated, however, that information relating to social media may be relevant to litigation. One court, for example, granted a defendant’s motion, which sought data from Myspace and Facebook, some of which was private. Another judge was willing to create a Facebook account in order to review information, and found certain information to be relevant to the case. Yet another court recognized that information contained in a person’s Facebook account could be subject to discovery in litigation, and ultimately allowed discovery of relevant information. In doing so, the court acknowledged a previous decision on the scope of discovery of social media, stating, “[t]he Court recognizes that the scope of discovery into social media sites ‘requires the application of basic discovery principles in a novel context,’ and that the challenge is to ‘define appropriately broad limits . . . on the discoverability of social communications.’”

Rule 34(a)(1) requires the production of documents and electronically stored information that are within a party’s “possession, custody, or control.” Recent court decisions have indicated that while information stored in the cloud may not be within a party’s direct “possession” or “custody,” courts are likely to view it as being within a party’s “control,” and courts have held parties responsible for producing such data. In assessing control, many courts have applied a “practical ability” test, where a litigant is found to be in control of data in question, regardless of legal entitlement to that data, as long as the litigant had the practical ability to obtain

17 Blank, supra note 13 at 496.
21 Id. (quoting EEOC v. Simply Storage Mgmt., 270 F.R.D. 430, 434 (S.D.Ind. 2010)).
22 FED. R. CIV. P. 34 (a)(1).
it. Some courts have used a “practical ability” test to evaluate spoliation claims, applying the test in the context of production and preservation obligations. Courts have required parties to allow full access to computers or servers rented from third parties, treating them the same as those within a party’s possession.

A number of cases find that electronically stored information in the hands of a third party is within the “control” of the litigant. In *Columbia Pictures v. Bunnell*, for example, the defendant claimed that it could not meet a discovery demand, because a third-party provider stored the data in question. The court disagreed, finding that while the defendant might not have possession of the data, the defendant still had custody or control of the data, since the defendant had rerouted data onto the third-party servers from its own servers. In *Tomlinson v. El Paso Corp.*, the court also found that an employer was in possession, custody, or control of electronic data in actual possession of a third-party provider, since the employer was required by law to maintain the records in question, and the employer could not delegate its duties to a third party. In *Flagg v. City of Detroit*, the court disagreed with the contention that the

---


24 *See Cross & Kuwahara, supra* note 2 at 3 (citing *In re NTL, Inc. Securities Litigation*, 244 F.R.D. 179, 195 (S.D.N.Y. 2007)).


27 *Id.*

Stored Communications Act prohibited the production of electronic communications stored by nonparty providers, and allowed discovery to go forward.\textsuperscript{29}

This willingness to allow discovery from the cloud is not limitless, however. Considerations of relevance, undue cost, and privacy will influence whether discovery of social media and data in the cloud is appropriate.

First, while discovery of social networking data might be appropriate in some circumstances, courts will weigh the relevance of such data before compelling discovery.\textsuperscript{30} In \textit{Mackelprang v. Fidelity National Title Agency of Nevada, Inc.}, the court denied Fidelity’s motion to compel production of private messages that Mackelprang had sent via her Myspace accounts.\textsuperscript{31} Mackelprang alleged sexual harassment, and Fidelity sought discovery of the messages, believing they would provide evidence that Mackelprang was involved in extra-marital affairs, in an effort to impeach her credibility.\textsuperscript{32} The court denied the motion to compel, stating that Fidelity’s ability to compel should be limited to messages that directly related to Mackelprang’s employment.\textsuperscript{33} In \textit{T.V. v. Union Township Board of Education}, the plaintiff moved for a protective order, barring the defendant from seeking discovery from the

\begin{footnotesize}
\begin{itemize}
    \item \textsuperscript{29} 252 F.R.D. 346, 349-50 (E.D. Mich. 2008).
    \item \textsuperscript{30} Blank, \textit{supra} note 13 at 498.
    \item \textsuperscript{31} 2007 WL 119149, (D. Nev. Jan. 9, 2007).
    \item \textsuperscript{32} \textit{Id.} at *3.
    \item \textsuperscript{33} \textit{Id.} at *8.
\end{itemize}
\end{footnotesize}
plaintiff’s online social networking profiles, on the basis of privacy rights and undue burden. The court granted the protective order, although it did allow for the possibility of allowing later discovery if the defendant could show sufficient relevance.

Second, and closely related, Rule 26(b)(2)(B) limits discovery, even of data within the party’s possession, custody, or control, when the production of that data would impose undue burden or cost on the producing party. If it would be too difficult or expensive to produce the data in a useable form, then the cost must be balanced against the production’s relevance to the case. Courts may consider different types of computer data more or less accessible, and the form of the data in question could weigh into the balance of determining whether it would be an undue burden for a party to produce it. While there is no guarantee, courts may be somewhat sympathetic to litigants facing discovery problems with preserving or producing data in possession of third-party cloud providers, when obtaining that data would cause an undue cost or burden. In one case, for example, while the court did find that Proctor & Gamble had a legal right to obtain data located on a third-party server, the court also found it was an undue burden, as Procter & Gamble would have either had to purchase a costly mainframe or pay the third-party $30 million in order to obtain that data, which had been altered due to routine updates to the database. While Rule 26(b)(2)(B) may present some hope to litigants, a claim

---

35 Id.
37 Id.
39 See Cross & Kuwahara, supra note 2 at 9 (discussing Proctor & Gamble Co. v. Haugen, 427 F.3d 727, 739 (10th Cir. 2005)).
that data located in the cloud is not reasonably accessible may be met with skepticism, given the relative ease with which certain cloud providers may be able to preserve or produce data.\footnote{Cross & Kuwahara, supra note 2 at 12.}

Third, another important consideration in the discovery and production of information pertaining to social media accounts is an individual’s privacy interests. The trend in case law suggests that individuals’ private postings through social media sites will not be afforded a great deal of privacy protection by the courts.\footnote{Thomas I. Barnett & Kenneth R. Shear, \textit{The social media networks: Issues in communications disclosure and preservation}, 1 \textit{INTERNET LAW AND PRACTICE} § 10:13 (2011).} In \textit{EEOC v. Simply Storage Mgmt.},\footnote{\textit{EEOC v. Simply Storage Mgmt.}, supra note 28.} the court stated that while privacy concerns may play into whether a discovery request is overly burdensome or relevant, a person’s expectation of privacy, with regard to social networking profiles, is not itself a “legitimate basis for shielding those communications from discovery. . . . [M]erely locking a profile from public access does not prevent discovery either.”\footnote{\textit{EEOC v. Simply Storage Mgmt.}, supra note 28.}

Nevertheless, courts have offered contrasting views on whether to grant employers’ discovery requests relating to an employee’s password-protected email or social media accounts, when those accounts were accessed from work computers. In \textit{McLaren v. Microsoft Corp.},\footnote{\textit{McLaren v. Microsoft Corp.}, No. 05-97-00824-CV, 1999 WL 339015, at *4-5 (Tex. App. May 28, 1999).} for example, the court ruled that an employee did not have a reasonable expectation of privacy with regard to personal password-protected emails, since he had stored those emails on a work computer. In contrast, the court in \textit{Stengart v. Loving Care Agency, Inc.} did not allow employers to access an employee’s web-based email account, even though it had been
accessed from a work computer. The court stated that employers should have access only to communications that had an “impact on its business or reputation,” such as when an employer wishes to access communications to analyze whether an employee’s lack of productivity may warrant disciplinary action. Companies should therefore be aware that a court might still be reluctant to rule against an employee’s right to privacy.

Courts are determining on a case-by-case basis whether a person’s claim of privacy is reasonable. In Harding Lawson Associates v. Superior Court, a Court of Appeal found that in weighing a litigant’s right to information against an opposing party’s need for confidentiality, employee privacy should be favored unless “the litigant can show a compelling need” for the documents in question, and the information cannot otherwise be obtained. In McMillen v. Hummingbird Speedway, Inc., the plaintiff objected to discovery of his private posting on Facebook and Myspace. Looking at the terms of service, the court ultimately concluded that these sites could access all user posts, private or public, and that the terms of service allowed those networks to disseminate postings when deemed appropriate, thus negating the expectations that a “private” posting would actually be private or confidential.

In sum, to date, courts have not arrived at a clear-cut consensus concerning the electronic production of data relating to social media. Discovery obligations involving cloud computing must be evaluated on a case-by-case basis. There is not an overarching

---

45 Id.
46 Id. at 401.
49 Id. at *1–2.
framework that can be uniformly and widely applied. Each case will call for a balance of benefits and risks to the discovery of
documents or data relating to cloud computing, including social media. In balancing these risks and benefits, legal considerations
include relevance, cost and burden, and privacy.

III. STRATEGIES AND BEST PRACTICES FOR COMPANIES REGARDING THIRD PARTY CONTRACTED
CLOUD-COMPUTING SERVICES

The relationship that a company has with the cloud provider can greatly impact that company’s ability to comply with
discovery obligations during litigation, in terms of the company’s ability to preserve and produce the necessary data. While some
third-party cloud services providers may expressly outline obligations related to electronic discovery, other providers may have
contracts limiting their obligations, which could cause problems for a company during litigation.\textsuperscript{50} Companies may also have a very
limited contractual relationship, in the case of free social media services such as Google applications, Facebook, or other platforms,
where the only contract between the parties is that service’s standard terms of agreement.\textsuperscript{51} Yet in each of these situations, where third
parties may be in possession of data that is relevant to litigation, the primary company or individual involved in the litigation may still
face electronic discovery obligations to preserve and produce that data.\textsuperscript{52}

\textsuperscript{50} David D. Cross & Emily Kuwahara, \textit{E-Discovery and Cloud Computing: Control of ESI in the Cloud}, EDDE JOURNAL, Spring 2010, at 2, \textit{available at}
\textsuperscript{51} \textit{Id.} at 2-3.
\textsuperscript{52} \textit{Id.} at 3.
To begin to address the issues presented by cloud computing and social media, litigants should be aware of heightened discovery issues that pertain to data stored in the cloud. In this section, I highlight nine key issues.

First, it is important to begin by assessing the total costs and benefits of cloud computing. While the cost of storing data in the cloud may be lower, it could actually result in much higher production costs. Lower initial costs could lead to the retention of more data over a period of time, which would result in higher costs to review larger volumes of data during the discovery process. Additionally, complexities in the preservation and collection of this data could further increase discovery costs.

Second, in situations where companies are contracting third-party providers for cloud computing services, it is important to consider various information management issues up front. What will the provider do to permit its clients to manage their own data? How will it comply with the different retention periods required for different record categories? Clients of cloud solutions should consider the relative difficulty they could have in meeting record retention obligations, as many cloud solutions do not include record functions. Companies should also consider whether the links between records and their metadata are adequately preserved.

Third, in selecting providers, companies must consider the third-party providers’ policies and practices with respect to routine deletion of data. Cloud providers may have servers that routinely delete or override data that a party may ultimately be responsible for preserving. Companies should be aware of whether the cloud computing services include an automatic purge of data after a certain period of time, and whether the automatic purge function can be turned off entirely, or in a targeted fashion, if and when necessary for

---

53 In addition to the general requirements of the Federal Rules of Civil Procedure, regulatory language specifies that retention and preservation duties apply to certain social media. According to FINRA Regulatory Notice 10-06, any company that “intends to communicate, or permit its associate persons to communicate, through social media sites must first ensure that it can retain records of those communications as required by Rules 17-a-3 and 17a-4 under the Securities Exchange Act of 1934 and NASD Rule 3110.”
adequate retention. It may also be important to note who controls those functions, and to what extent. There may be no way for a party to preserve data and subsequently produce it when a nonparty provider has deleted it in the course of routine operations.\footnote{Cross & Kuwahara, supra note 2 at 7.} For this reason, companies should also make sure they understand the backup policies of the cloud providers, to make sure such policies are adequate.

Fourth, it is important to think carefully about putting anything in the cloud that one would not want a competitor or litigant to see. Once information is in the cloud, it may be difficult to control what information gets produced. This can result in the production of privileged, confidential or protected information. To minimize the risk of disclosure of a client’s data without any notice, clients of cloud service providers should also consider negotiating contract provisions obligating the providers to notify the clients, to the extent permitted by law, in the event that government agencies or other third parties directly subpoena cloud services providers for information. Such notice would provide clients with an opportunity to contest the production, if necessary.

Fifth, it may be necessary to separately retain data from high-risk personnel, such as senior management, as well as possibly finance and legal departments. While companies may be able to encrypt potentially sensitive data from these sources in the cloud, cloud providers may be compelled to disclose relevant encryption keys.

Sixth, in order to mitigate the cost and size of document productions, companies may consider avoiding using the cloud for backups of certain unique data. This will reduce the likelihood of having to extract that data from cloud providers’ backups for discovery purposes.
Seventh, some cloud services have limited ability to preserve and extract data when necessary for litigation. Companies may consider using the litigation hold features of other software as an alternative, in order to ensure adequate preservation of documents. Companies can elect to use a “hosted email archiving service, as well as other platforms that allow users to retrieve relevant emails, like Google Message Discover and Microsoft Office 365. There are pros and cons to taking such approaches, which need to be analyzed carefully. It should also be noted that, while these programs provide a way to preserve emails, it can be more difficult for companies to preserve and pull other cloud-based documents. Companies should be aware that they may face challenges accessing versions of documents stored in cloud-based applications, like Sharepoint and GoogleApps, for discovery purposes.

Eighth, in the event that data collection is necessary, companies must consider who will be responsible for the data extraction. Procedures for data extractions should be incorporated into agreements with cloud providers, to the extent feasible, so that companies can ensure adequate coverage of their future needs. Companies should also seek to ensure that they incorporate procedures for data searching into their provider agreements, and account for costs of extraction and searches of data when making the decision of what to move into the cloud. In addition, there should be a clear understanding of how confidential, trade secret and privileged materials will be protected, and how security will be maintained. If the cloud provider cannot offer its clients an adequate solution, companies may need to use third parties to handle data extractions. If third parties will be assisting, companies should ensure that there are adequate quality control and chain of custody procedures in place.

---

55 Id.
56 Id.
Finally, in situations where there is no contractual remedy, where the provider refuses to comply, or where the data is subject to statutory protections, it may be necessary to subpoena the providers for the data. Companies should carefully document any and all attempts to preserve or produce data that is stored in the cloud, as a way to try to avoid or mitigate any court sanctions for spoliation of relevant data, in the event that third parties in possession of the data prove uncooperative.

IV. STRATEGIES AND BEST PRACTICES FOR COMPANIES REGARDING THE USE OF SOCIAL MEDIA PLATFORMS

Companies may have even less control over information stored in the cloud that is outside of the realm of contracted third-party cloud services providers. Information in the cloud as a result of the use of social media platforms presents additional difficulties in managing document production and data extraction, processing, and analysis. In contrast with contracted cloud service providers, companies cannot tailor their relationships with the major social media platform providers in order to adequately protect their interests. Twitter, one of the most popular social media platforms, for example, provides a disclaimer that services are available “AS-IS”. Companies must therefore find other strategies for mitigating their risks.

57 Cross & Kuwahara, supra note 2 at 10.
58 Id.
59 Twitter, Twitter Terms of Service, at http://twitter.com/tos (last visited Nov. 28, 2011).
Companies should have clear policies set in place in order to mitigate liability with regard to an employee’s use of social media sites. Companies should also be sure to clearly notify all employees of these policies, in order to reduce potential complications surrounding the issue of employee privacy.

First, companies should consider banning any personal or objectionable use with workplace computers. Employers may also limit the use of social media on workplace computers by blocking certain sites, and should have carefully crafted policies in place prohibiting the use of a company’s official email address when registering on external social media sites. Employers should also limit employees from using certain trademarks or logos without prior approval, posting business documents or other business information that has not been publicly released, and posting information about customers or suppliers without their prior permission. Employers can also have policies in place requiring individuals who create social media sites relating to the company to include a disclaimer that the site is not an “official company site.”

Second, companies should consider making clear to employees that they will monitor an employee’s activity on any workplace or company computer and email, which can be accomplished through monitoring and time-stamping software tools. When a company has such policies in place, a court may be more likely to take the view that an employee’s expectation of privacy is diminished. For example, in In re Asia Global Crossing, Ltd., the court, in assessing an employee’s expectation of privacy, considered whether the
corporation maintained a policy banning personal use, whether the company monitored the use of the employee’s computer or email, whether the employee was aware of any monitoring policies, and whether third parties had a right to access the computer or emails.\footnote{322 B.R. 247, 257 (S.D. N.Y. 2005).}

In developing policies for employees, however, a company must be careful not to overstep legal boundaries. While companies may wish to limit the types of information disseminated by employees on social networking sites, companies must recognize that certain types of communications may be protected by law. For example, Section 7 of the National Labor Relations Act (the “NLRA”) restrains employers from interfering with, restraining, or coercing employees in exercising their rights to self-organize, form, join, or assist unions.\footnote{29 U.S.C. §157 (2000).} For example, employers may not discipline employees for continuing, in an online forum, concerted activities that began at work.\footnote{29 U.S.C. §158(a)(1).} Employers should also be cautious about enacting or enforcing any overly broad social media policies, as they may draw the attention of the NLRB, and may violate Section 8(a)(1) of the NLRA.\footnote{Id.}

V. CONCLUSION

Companies are increasingly facing electronic discovery issues pertaining to cloud computing and social media. As cloud computing and social media grow in popularity, so will the likelihood that a company will face electronic discovery demands as a result. Companies should be aware of potential issues and responsibilities, and do whatever possible to address potential problems
before they arise. Otherwise, companies may later find themselves facing expensive discovery problems or even court sanctions as a result of difficulties arising from the preservation and production of data from the cloud.
Hold it! Avoiding an Electronic Discovery Disaster with Effective Litigation Holds:

Elizabeth S. Fenton
Diana Rabeh
Reed Smith LLP
Wilmington, Delaware

Jonathan M. Shapiro
Shapiro Law Offices, LLC
Middletown, Connecticut
HOLD IT! AVOIDING AN ELECTRONIC DISCOVERY DISASTER WITH EFFECTIVE LITIGATION HOLDS

Elizabeth S. Fenton
Diana Rabeh
Reed Smith LLP
Wilmington, Delaware

Jonathan M. Shapiro
Shapiro Law Offices, LLC
Middletown, Connecticut
I. Introduction

206,000,000 barrels: The U.S. government's estimate of how much oil flowed from the explosion of BP’s rig into the Gulf of Mexico.¹ $1,600,000,000: BP’s confirmed cost of the Deepwater Horizon oil spill, as of December 1, 2010. 1,000,000,000,000 bytes. The amount of data in the form of documents, emails, voicemail, text messages and instant messages expected to be retrieved from BP’s electronic discovery.² The sheer volume of electronic data will cause the Deepwater Horizon oil spill to become one of the largest electronic discovery events in history.

In the wake of events like an oil spill, natural disaster, or other catastrophic event, clients find themselves confronting urgent duties regarding the maintenance and preservation of electronic evidence, duties that may possibly burden their ability to conduct operations going forward. As litigators, especially as business torts litigators, it is imperative that we provide effective guidance to clients both before and during litigation to ensure that these duties are met and to minimize—to the degree possible—the burden on their business so that a disaster does not become an e-discovery disaster as well. In this article, we will rely on recent case law and guidance from the Sedona Conference to discuss the kinds of policies and procedures that ought to be in place before litigation is reasonably anticipated, and then how to implement a litigation hold which focuses on data preservation, collection and backup tape remediation for large amounts of data.

Although the explosion of electronic discovery over the years alone warrants heavy emphasis on having a proper system in place to respond to pending or anticipated litigation, a disaster such as the Deepwater Horizon oil spill reminds us that work done before a crisis will pay off when the inevitable crisis comes. In the face of an overwhelming amount of daily electronic communication and the relative ease of spoliation, we must advise our business clients of the triggers for the common law duty to preserve evidence and assist them in developing policies and practices to ensure that the duty is met when it arises.
We must also advise them that the high costs associated with electronic discovery coupled with the risks of sanctions in the event of data destruction, even inadvertent destruction, make ignoring such a duty perilous.

II. The Law Governing Litigation Holds

A litigation hold is simply a communication within a company which requires that all information—whether paper or electronic—relating to the subject of a current or impending litigation be preserved for possible production in the litigation. The 2003 landmark case, Zubulake v. UBS Warburg, 202 F.R.D. 212 (S.D.N.Y. 2003), popularized the use of the litigation hold to satisfy preservation obligations imposed on parties. The Court explained that “[o]nce a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’” to safeguard all relevant data.3

“[W]hile a litigant is under no duty to keep or retain every document in its possession, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.”4 The purpose of a litigation hold is to prevent the automatic destruction of potentially relevant or discoverable documents and information pursuant to a document retention policy.

Amendments to the Federal Rules of Civil Procedure that took effect on December 1, 2006 codified the evolving obligation for companies to preserve, collect and produce “electrically stored information.” Except for a Note to Rule 37(f) which references the use of a “litigation hold” as a method of implementation, the Federal Rules do not define the scope of the preservation obligation under a litigation hold per se and do not expressly require litigants to adopt a “litigation hold.” Similarly, although the Delaware Court of Chancery recently issued guidelines regarding the preservation of electronically stored information, few other courts have done so.5 Nonetheless, many district courts have determined that the “utter failure to establish any form of litigation hold at the outset of litigation is grossly negligent” and
subject to sanctions. As one judge recently explained “[b]y now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records-paper or electronic-and to search in the right places for those records, will inevitably result in the spoliation of evidence.”

III. **When is the Duty to Preserve Triggered?**

Because the duty to preserve is not necessarily triggered at the commencement of litigation, it is imperative that a company is aware of when the duty to preserve documents and issue a litigation hold arises. “The duty to preserve material evidence arises not only during litigation but also extends to the period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.”

When the duty to preserve is triggered, a party must take reasonable steps to preserve relevant and/or discoverable information, which includes, “what it knows, or reasonably should know is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.”

A party who fails to preserve and produce information as required may be subject to a range of sanctions.

Although this rule may appear to be straightforward, its application can be hard to pin down and difficult to determine in some situations. For example, when an unexpected disaster strikes, many would argue that the duty to preserve arises almost immediately at the outset of the disaster. At least one commentator has speculated that the duty to preserve arguably arises before disaster strikes, particularly where the disaster is “man-made” or the result of ongoing negligence.

Suffice it to say that “[d]etermining whether a duty to preserve is triggered is fact-intensive and is not amenable to a one-size-fits all or a checklist approach.”

The Sedona Conference, recognizing that determining when the duty to preserve is triggered can be difficult, has provided a number of guidelines to practitioners. First, the Sedona Conference defines “reasonable anticipation of litigation” as arising “when an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when
it takes specific action to commence litigation.”14 This determination “should be based on a good faith and reasonable evaluation of relevant facts and circumstances.”15 Important reasonable facts and circumstances for a company to consider include:

1. The nature and specificity of the complaint or threat;
2. The party making the claim;
3. The business relationship between the accused and accusing parties;
4. Whether the threat is direct, implied or inferred;
5. Whether the party making the claim is known to be aggressive or litigious;
6. Whether a party who could assert a claim is aware of the claim;
7. The strength, scope, or value of the known or reasonably anticipated claim;
8. Whether the company has learned of similar claims;
9. The experience of the industry, and
10. Reputable press and/or industry coverage of the issue either directly pertaining to the client or of complaints brought against someone similarly situated in the industry.16

Accordingly, because the duty to preserve documents may arise well before a complaint has been filed or a subpoena is served, a company must be cognizant of the factors outlined above and must consider the necessity of a litigation hold whenever a claim or threat of a claim first comes to light.

IV. Avoiding an Electronic Discovery Disaster: Best Practices for Implementing Litigation Holds

Companies should not wait until disaster strikes or litigation is commenced to start thinking about how best to manage and protect their electronic data. The following practice tips are designed to assist companies in managing, storing and protecting electronically stored information and implementing a proper litigation hold.

1. Be Prepared. Before drafting a litigation hold policy, a company should set forth a “policy or practice setting forth a process for determining whether the duty to preserve information has attached.”17 As the Sedona Conference explained “adopting and consistently following a policy or practice governing an organization’s preservation obligations is one fact that may demonstrate reasonableness and good faith.”18 In addition, a company must know how its electronic data is stored, backed-up and archived so that it can draft a proper litigation hold policy. Specifically, companies should be aware of the potential “evidence destroyers” and problem areas such as automatic deletion of e-mail,
recycling backup tapes, upgrading and reformatting systems, laptop computers, home computers, portable storage devices such as flash drives and personal e-mail accounts.

2. **Be Proactive.** Businesses should periodically review and monitor their document retention policies before a situation necessitates the implementation of a litigation hold. By being proactive, a company can determine if there are any holes or deficiencies in the policy or its implementation and whether the policy needs to be updated. This step is also critical to a later showing of good faith, as Rule 37(e) provides that “[a]bsent 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.”\(^{19}\) The protection of this provision may be lost, however, if—after the duty to preserve is triggered—the retention policies are not suspended or modified.

3. **Set up an Electronic Discovery Team.** For larger companies and/or legal departments, the time and resources dedicated to putting together an e-discovery team are well worth it. This team should consist of not only legal personnel but technology personnel as well. Technology personnel will be particularly important for ensuring the suspension of any automatic deletions of e-mail, recycling backup tapes, and upgrading and reformatting systems. It is also important to designate and train a member of the electronic discovery team to handle inquiries from employees about claims or threats of litigation, the duty to preserve, and other questions regarding the litigation hold.

4. **Identify Key Players.** When litigation is reasonably anticipated, a business must quickly implement an effective litigation hold and make sure all sources of potentially relevant information are identified and placed on hold. In order to do so, a company must identify and interview the key players in the litigation as quickly as policy. It is important to note that it may be necessary to extend the litigation hold beyond the key players to “appropriate date stewards, records management personal, information technology (IT) and other potentially knowledgeable personnel.”\(^{20}\)
5. **Issue Effective Litigation Hold Policy Promptly.** When a company issues this hold notice, the company should disseminate it to its employees both electronically and via inter-office mail. The litigation hold should also include the following information: (1) description of the case in laymen’s terms; (2) instruction of which documents should be preserved and how such documents should be preserved; (3) instruction that any automatic deletions of e-mail or other electronic media should be suspended; (4) instruction that the recipient search all information for anything relevant or potentially relevant to the claim, and to err on the side of preserving; (5) explanation to recipients about the risk to the company and its employee for failing to heed the litigation hold request; and (6) contact information for the designated person from the e-discovery team, or an in-house or outside lawyer. The widespread use of electronic discovery makes it vital for litigants to employ litigation holds as soon as a claim or potential claim is reasonably anticipated. The failure to timely implement a litigation hold may not only result in spoliation but may be costly to a party in the form of court-ordered sanctions, including the entry of a default judgment. One court even went so far as to suggest the imposition of jail time for spoliation. Businesses cannot afford to take the requirement that they issue litigation holds lightly.

6. **Be Over-Inclusive.** It doesn’t hurt to be over-inclusive in determining which documents should be placed in the litigation hold and employees should always err on the side of caution. Although preserving and collecting massive quantities of data can be expensive, this cost must be weighed against the very real threat of spoliation and issuance of sanctions. Thus, until a company is aware of what discovery requests it will face in the future, it is recommended that companies preserve their data very broadly.

7. **Be in Control.** It is necessary not only to implement a litigation hold but also to continually take affirmative steps to monitor compliance. The monitoring and testing of its litigation hold policy ensures that employees are following the policy and its data has been safeguarded. In *Zubulake*, the court explained that litigation hold responsibilities do not end with the issuance of the litigation hold: “Counsel must oversee compliance with the litigation hold, monitoring the party’s efforts to retain and
produce the relevant documents."22 This is especially true where a company may face criminal charges, and employees may be tempted to delete or alter information that might get them in trouble. Throughout the process, counsel should document the steps taken to both ensure compliance and prevent the destruction of potentially relevant electronically stored information.

8. **Keep Communications Open.** A company should communicate with its employees to ensure that the litigation hold has been effectively implemented, while counsel is, at the same time, having ongoing conversations with opposing counsel and the court on the status and progress of electronic data. This is especially true where discovery may involve particular areas of sensitivity.

V. **Conclusion**

No one can predict when disaster will strike. But a company can and should prepare itself in the event that disaster unfortunately bestows upon it and take steps to minimize the risk of the occurrence of secondary electronic discovery disaster. As litigators, we play an instrumental part in ensuring that our business clients are prepared, if and when disaster strikes. In order to adequately prepare our clients and provide effective guidance, we must follow the best practices outlined above for implementing an effective litigation hold policy. The high costs of electronic discovery, as well as the risk of sanctions in the event of spoliation, even inadvertent, make it imperative that we assist our clients in proactively implementing policies and practices to ensure that the common law duty to preserve is met.

Elizabeth S. Fenton is a partner and Diana Rabe is an associate at Reed Smith LLP in Wilmington, Delaware. Jonathan M. Shapiro is a partner with Shapiro Law Offices, LLC in Middletown, Connecticut.


3 *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003); see also *ACORN (N.Y. Ass’n of Cmty. Org. for Reform Now) v. County of Nassau*, No. 05-2301, 2009 WL 605859, at *2 (E.D.N.Y. Mar. 9, 2009) (explaining that once the duty to preserve arises, “a litigant is expected, at the very least, to suspend its routine document and retention/destruction and to put in place a litigation hold” (internal citation omitted)).


8 *Silvestri v. General Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001); see also *Jacob v. City of New York*, No. 07-cv-04141, 2009 WL 383752, at *1 (E.D.N.Y. Feb. 6, 2009) (“[The] obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.”).

9 See *Wm. T. Thompson*, 593 F. Supp. at 1455.
“Sanctions may be imposed against a litigant who is on notice that documents and information in its possession are relevant to litigation, or potential litigation, or are reasonably calculated to lead to the discovery of admissible evidence, and destroys such documents and information.”


Id. at 269.

Id. at 270.

Id. at 276.

Id. at 274.

Id.

Id. at 283.

See Sean T. Carnathan, *Jail Time for Spoliation?*, ABA Litigation News, November 29, 2010, http://www.abanet.org/litigation/litigationnews/top_stories/112910-spoliation-extreme-sanctions.html. In *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497 (D. Md. 2010), Magistrate Judge Paul W. Grimm of the U.S. District Court for the District of Maryland, determined that defendant’s willful acts of spoliation warranted not only partial default judgment in favor of plaintiff but also constituted civil contempt. *Id.* at 500. The Court ordered the culpable individual defendant to be “imprisoned for a period not to exceed two years unless and until he paid pays to Plaintiff the attorney’s fees and costs” allocable to spoliation. *Id.* (internal citations omitted). In later proceedings, U.S. District Judge Marvin J. Garbis
modified the sanctions to eliminate the potential for jail time, reasoning that it was not appropriate to order the individual “[d]efendant incarcerated for future possible failure to comply. . . .” See Victor Stanley, Inc. v. Creative Pipe, Inc., D.C. Md., C.A. No. MJG-06-2662, Garbis, J., at *3 (Nov. 1, 2010) (Memorandum and Order).

22 Zubulake, 229 F.R.D. at 432.