GIBSON DUNN

July 15, 2015

2015 MID-YEAR E-DISCOVERY UPDATE

To Our Clients and Friends:

Progress on Some Fronts, But Significant Dangers Remain, and New Dangers Emerge

E-discovery remains an incredibly rich and rapidly developing field, as the many developments on which we report from just the first half of 2015 attest. We are seeing progress in some areas (*e.g.*, predictive coding, cost recovery, and rule amendments), remaining dangers in others (*e.g.*, sanctions, preservation, and cross-border discovery), and new dangers emerging (*e.g.*, text messaging, mobile devices, and e-discovery vendor selection).

We encourage you to read all the content below, but we recognize there is a lot. So, you may want to approach it one topic at a time.

Our 2015 Mid-Year E-Discovery Update covers the following (click on headings to go to full section):

- **Text Messaging and Mobile Devices:** Text (aka instant) messaging and mobile devices are shaping up to be the new frontier in e-discovery. Texts and instant messages are increasingly at issue in investigations and litigation. But extracting them from mobile devices can be expensive and time consuming, if possible at all. Consequently, companies should consider implementing appropriate controls over employees' business-related text and instant messaging, particularly on mobile devices.

- **Information Governance:** Information governance (or "IG") has been the "next big thing" in e-discovery over the past couple of years. Like all "next big things," the early breathless hype about "IG" is beginning to fade. Companies are eschewing grand plans to implement information governance programs on every nook and cranny of their information systems, and are instead focusing on high-yielding, low-hanging fruit such as email and disposing of legacy backups.

- **The Internet of Things:** "IoT" is being promoted by some in the e-discovery world as the next, next big thing. To us, it seems to require a rather fertile imagination to identify circumstances where IoT data would be relevant to most business disputes. Nevertheless, companies should consider the legal significance of the IoT data in their possession, custody or control and, if determined to be necessary, have a process in place for preserving and extracting this data, should the need arise.

- **Predictive Coding:** Predictive coding continues to be the big underachiever of e-discovery. There may be a number of reasons why it is not being utilized more, despite its potential to

significantly reduce the costs and time required for document review. One, for certain, has been the perception that disclosing irrelevant documents and coding decisions from training sets will be required of those who wish to use predictive coding. Magistrate Judge Andrew Peck of the Southern District of New York has sought to dispel that perception in *Rio Tinto PLC v. Vale S.A.*, in which he identifies a number of more palatable alternatives that make such disclosure unnecessary.

- **Sanctions:** Sanctions are an ever-present danger in the e-discovery world. Continuing a trend that we have seen in recent years, sanctions were imposed not only for spoliation--*i.e.*, failing to preserve relevant information after a duty to preserve arose--but also for delayed productions of relevant and responsive information.

- **Preservation:** Courts issued several interesting decisions in the first half of 2015 regarding (1) the trigger of the duty to preserve, (2) the extent to which the duty reaches data in the possession of non-parties, and (3) the subject matter scope of the duty.

- **E-Discovery Cost Recovery:** Prevailing parties increasingly are seeking to recover a portion of their e-discovery costs upon conclusion of their litigation pursuant to 28 U.S.C. § 1920(4), which permits the taxing of "[f]ees for exemplification and the costs of making copies of any materials where the copies are necessarily obtained for use in the case." Courts are increasingly granting recovery of e-discovery costs beyond just those related to the conversion of electronic documents to TIFF format.

- **Discovery of Social Media:** Reflecting that the use of social media continues to proliferate in business and social contexts, and that its importance is increasing in litigation, the number of cases focusing on the discovery of social media continued to skyrocket in the first half of 2015. Courts are still struggling to develop rules and protocols applicable to social media evidence, including whether special authentication rules should govern social media evidence, what threshold showing of relevance must be made before discovery should be allowed, when the duty to preserve social media evidence arises, what role privacy rights should play in social media discovery, and who should bear the burden of review.

- **Governmental Investigations:** Courts continue to grapple with how to apply e-discovery concepts to governmental investigations. For example, courts have had to balance Fourth Amendment rights with the opportunities for discovery created by the Stored Communications Act (SCA), 18 U.S.C. §§ 2700 *et. seq,*, which permits access to the files of technological intermediaries, such as Internet service providers and cell phone providers.

- **E-Discovery Vendor Developments:** With respect to e-discovery service providers (aka vendors), in some respects it is the best of times and in others it is the worst of times. Much of the market is immature, with a dizzying array of vendors and consumers not well equipped to distinguish among them. Aggressive sales tactics are common, and attempts at consumerizing e-discovery technology and services are a troubling new trend.

- **Federal Rule Amendments:** It has taken an interplanetary probe nine and one half years to travel to Pluto, so the five years that the latest e-discovery amendments to the Federal Rules of Civil Procedure have taken to come to fruition seems pretty good in comparison (by cosmic standards, at least). The Supreme Court approved their adoption in April, leaving Congress as the only potential obstacle to their implementation in December (what possibly could go wrong?). The sanctions rule amendment may make a significant difference, so the wait will likely be worth it.

- **International E-Discovery Developments:** The cross-border transfer and disclosure of information remains challenge for multinational corporations. The proliferation of data localization laws such as China's State Secret laws have led companies and their counsel to increasingly process and review documents locally. In Europe, the EU-US Safe Harbor Framework, which allows certified US companies to transfer personal data outside Europe if they meet certain requirements, is being amended with the goal of stricter compliance with EU data privacy provisions. At the same time, the Framework's adequacy is being challenged before the European Court of Justice.

Text Messages and Mobile Devices

Text (aka instant) messaging and mobile devices are shaping up to be the new frontier in e-discovery. In 2013, the Pew Research Center reported that 91 percent of American adults owned a mobile phone and 81 percent used their phone to send or receive text or instant messages. *See* Pew Research Center, *Cell Phone Activities 2013* (Sept. 16, 2013). An open question, however, was how often text messaging is used for business-related communications. A RingCentral survey found that 79 percent of respondents used text messaging for business purposes, and 32 percent had closed a business deal by text message. *See* Gareth Evans and Lauren Eber, *Is Instant Messaging The Next Email?*, Inside Counsel (Nov. 1, 2013).

Since then, text messages have increasingly played a role in high profile controversies. Relevant text messages are now more commonly sought in governmental and other investigations, and are occasionally at issue in civil litigation. Text messages sent and received on mobile device apps may feature an even greater degree of casual banter than emails. Users may engage in such casual communication assuming that their messages are "off the radar" because they are not going through company servers. Text messaging apps often store messages in databases on the mobile device, however, and "deleted" messages may still be extracted, though it can be expensive and difficult to do so (and such deleted messages are generally considered to be inaccessible). *See* Gareth Evans and Veeral Gosalia, *The Coming Storm: Companies Must Be Prepared to Deal With Text Messages on Employee Mobile Devices*, 15 Digital Discovery & e-Evidence (Bloomberg BNA, June 25, 2015).

Most often, text messages are not for business purposes and they are not relevant to the issues in litigation and investigations. But, occasionally they are, and as we reported in our 2014 Year-End E-Discovery Update, text messaging and mobile devices have increasingly become the subject of sanctions decisions. An example from the first half of 2015 is *Clear-View Technologies, Inc. v. Rasnick*, No. 13-cv-02744-BLF, 2015 WL 2251005 (N.D. Cal. May 13, 2015). Although primarily

focused on when the duty to preserve was triggered--the court held it was approximately two years before the suit was filed--the case is noteworthy for what the court found should have been preserved. The court sanctioned defendants for, among other things, having deleted relevant text messages and having "lost or thr[own] away" several mobile devices (including iPhones and an iPad) used to access relevant communications and documents. *See id.* at *5. The case reflects that where unique and relevant electronically stored information is contained in text messages and stored on mobile devices, courts increasingly will hold parties responsible for their preservation.

Companies may mitigate the risks associated with discovery of text messaging, including BYOD policies, implementing "sandboxes" (separate spaces for work apps) on employees' mobile devices, and requiring the use of enterprise texting apps that are journaled or backed up onto company servers. We expect preservation of relevant text messages and other data on mobile devices to be an increasingly common and important issue in the future. *See The Coming Storm*, *supra*, 15 Digital Discovery & e-Evidence (June 25, 2015).

Back to Top

Information Governance

Information governance has been the "next big thing" in e-discovery over the past couple of years. Like all "next big things," the early breathless hype about "IG" is beginning to fade as the next "next big thing" comes around the corner with its own trendy acronym ("IoT"--Internet of Things--anyone?). Early visions of grand information governance projects--including automated classification of documents for disposal using predictive coding algorithms--have, for the most part, not yet gained much traction in the business community.

IG was earlier conceived as an integrated approach to records management providing an overall framework for managing, organizing, and defensibly deleting data throughout an organization. It is a worthy goal whose time will likely come, eventually. In the meantime, companies are focusing their efforts on low hanging fruit that can provide bountiful harvests. The most prominent of these more attainable projects have consisted of implementing e-mail retention and defensible deletion policies, and defensible disposal of legacy backups.

In addition to retention and disposal programs, there is a growing trend towards adoption of "data minimization" policies, which can have practical benefits in both the legal and business spheres. Data minimization policies encourage employees to reduce the volume of data they generate--focusing on the front-end creation practices rather than the back-end storage and deletion practices. Such programs may not solve all the problems that IG seeks to address, but they may make a difference.

An important issue that has not yet received a lot of attention, but for which there is an increasingly pressing need to address, is the need to have enterprise controls--such as journaling and defensible disposal--applied to work-related text messages on mobile devices. Absent some form of information governance applied to employee texting, the risks of exploding litigation costs (extracting data directly from mobile devices is time consuming and expensive, if it works at all) and spoliation sanctions may increase considerably as more employees use texts for business-related messaging.

If there is a "next big thing" within information governance, addressing work-related text messaging on mobile devices should be it. *See* Gareth Evans and Veeral Gosalia, *The Coming Storm: Companies Must Be Prepared to Deal with Text Messages on Employee Mobile Devices*, 15 Digital Discovery & e-Evidence (Bloomberg BNA June 25, 2015).

Back to Top

The "Internet of Things"

One of the newest technological advances that could, hypothetically, complicate parties' preservation and collection obligations is the growing web of interconnected, data-receiving and data generating devices referred to as the Internet of Things (often referred to as the "IoT"). Indeed, in some e-discovery circles, the IoT appears to have become the NBT (that is, the "next big thing"), prominently included at the top of e-discovery discussion agendas, and joining the ranks of past breathlessly hyped topics such as early case assessment ("ECA"), discovery of ESI stored in the cloud, and information governance ("IG"). It is too soon to tell whether IoT will become truly important in significant corporate litigation and investigations, but we expect that it will be the relatively rare exception rather than the rule.

IoT has been described as an "ecosystem of interconnected sensory devices performing coordinated, pre-programmed--and often learned--tasks" that differs from the traditional Internet because it operates without the necessity for active human input. *See* Elizabeth McGinn & Ty Yankov, *Trading Beyond Fear: eDiscovery of the Internet of Things*, Electronic Commerce & Law Report, 20 ECLR 562, Apr. 15, 2015. Data-collecting sensors that feed into this network may one day become a part of daily life--take, for example, fitness-tracking devices that monitor vital signs, sending a constant stream of data to the cloud for storage and future analysis.

Additionally, many household items such as garage door openers, thermostats, alarm systems and appliances are already IoT enabled, with automobiles and medical devices soon to follow. According to a 2013 poll, 96 percent of surveyed senior executives said they expected their businesses to utilize IoT within the next three years. Clint Witchalls, *The Internet of Things Business Index: A Quiet Revolution Gathers Pace*, The Economist (Oct. 29, 2013).

IoT's implications for data preservation and collection are complicated due to the fact that this data is not "created" by humans, but rather by devices, with the data processed and stored on the cloud. One question courts are likely to have to address is who controls such cloud data for disclosure purposes--potential options are the device manufacturer, the party that monitors an individual's data, or the individual from whom the data is collected. Although the question of data control can largely be addressed by contracts between parties, there are likely to be at least some contracts that do not cover the issue, and courts will be left to decide based on applicable rules of civil procedure. Applying Federal Rule of Civil Procedure 34(a), which requires litigants to produce ESI that is in their "possession, custody, or control," courts may look to how a party uses the relevant data to determine if that party is "in control" of that data. *See Brown v. Tellermate Holdings, Ltd*., No. 2:11-cv-112, 2014

WL 2987051 (S.D. Ohio July 1, 2014) (plaintiff controlled cloud-based financial data). However, much remains to be seen in this emerging area.

Despite these issues, IoT should not yet strike fear into the hearts of business litigators. To us, it seems to require a rather fertile imagination to identify circumstances where IoT data would be relevant to a business dispute. Nevertheless, companies should consider the legal significance of the IoT data in their possession, custody or control and, if determined to be necessary, have a process in place for preserving and extracting this data, should the need arise.

Back to Top

Predictive Coding

The most important predictive coding case of the first half of 2015--*Rio Tinto PLC v. Vale S.A.*, 306 F.R.D. 125 (S.N.D.Y. 2015)--did not involve an actual dispute: the parties stipulated to a predictive coding protocol, which the court approved. Nevertheless, Magistrate Judge Andrew Peck wrote an opinion that provides significant guidance to litigants regarding the use of predictive coding (commonly referred to as "Technology Assisted Review" or "TAR," a nomenclature with which we are not particularly enamored, as there are various types of technology assisted review in addition to predictive coding).

Of particular significance, Judge Peck wrote in *Rio Tinto* that sharing training sets of documents--including the irrelevant documents in the training set and counsel's coding decisions on them--is not necessary to ensure that the predictive coding model was trained appropriately. Rather, Judge Peck pointed out that there are alternatives to producing the training documents and coding decisions. *See id.* at 128-129.

To understand the importance of this statement in *Rio Tinto*, it's helpful to know some of the backstory. Three years ago, in *Da Silva Moore v. Publicis Group*, Judge Peck issued the first published decision recognizing predictive coding as an "acceptable way to search for relevant ESI in appropriate cases." *Da Silva Moore v. Publicis Group*, 287 F.R.D. 182, 183 (S.D.N.Y. 2012). Predictive coding had been available for some time, but it generally wasn't being used.

Judge Peck knew that attorneys who were aware of predictive coding were nevertheless reluctant to use it because no court had approved it. Thus, he wrote in *Da Silva Moore* that "[c]ounsel no longer have to worry about being the 'first' or 'guinea pig' for judicial acceptance of [predictive coding]." *See id.* at 193. Judge Peck wrote that "[w]hat the Bar should take away from this Opinion is that [predictive coding] is an available tool and should be seriously considered for use in large-data-volume cases where it may save the producing party (or both parties) significant amounts of legal fees in document review." *Id.*

So what's happened since then? Despite Judge Peck's endorsement of predictive coding in *Da Silva Moore*, and the rulings of a significant number of other courts either encouraging or approving the use of predictive coding, it generally has not caught on--certainly not to the extent that many thought it would have after *Da Silva Moore*. Why? One commentator recently opined that it's not because of

software makers, vendors, judges, governmental investigators or clients, many of whom favor and promote its use, but rather it's due to litigation counsel "not understanding the value of TAR" in appropriate cases. *See* Geoffrey A. Vance, *Confessions of an E-Discovery Lawyer: We're Light Years Behind*, LegalTech News (June 23, 2015).

There may be some truth to this, but we think the story is more complex, as it does not reflect the role of opposing counsel, who have been known to seek to effectively preclude the responding party's ability to use predictive coding by demanding conditions that the responding party will likely find unacceptable (often referred to as the "TAR tax").

Probably the greatest impediment to the use of predictive coding has been the argument that the party seeking to use it should agree to share its coding decisions on the documents used to train the predictive coding model, including providing to the opposing party the irrelevant documents in the training sets. Indeed, a certain mythology has developed that the "transparency and cooperation" that commentators and courts have encouraged in connection with predictive coding means that a party *must* provide these irrelevant documents to the other side. *See, e.g.,* our discussion of the *Progressive v. Delaney* decision in our 2014 Year-End E-Discovery Update.

When many lawyers and clients hear that they may need to share documents that are not relevant to the litigation with opposing counsel, they want nothing to do with predictive coding. Many also consider counsel's coding decisions on the training set to be protected attorney work product. *See, e.g.*, John M. Facciola & Philip J. Favro, *Safeguarding the Seed Set: Why Seed Set Documents May Be Entitled To Work Product Protection*, 8 Fed. Cts. L.Rev. 1 (2015).

In *Rio Tinto*, Judge Peck has sought to resolve this divisive issue. First, he points out that the courts have developed a significant amount of comfort with predictive coding in the three years since *Da Silva Moore*. "[T]he case law has developed to the point that it is now black letter law that where the producing party wants to utilize TAR for document review, courts will permit it." *Rio Tinto PLC*, 306 F.R.D. at 127.

Second, he points out that predictive coding also can no longer be considered an "unproven technology." Judge Peck quotes the *Dynamo Holdings* decision of last year, in which the court stated that "In fact, we understand that the technology industry now considers predictive coding to be widely accepted for limiting e-discovery to relevant documents and effecting discovery of ESI without an undue burden." *Id.* (quoting *Dynamo Holdings Ltd. P'Ship v. Comm'r of Internal Revenue*, 143 T.C. 9, 2014 WL 4636526 at *5 (T.C. Sept. 17, 2014).

Third, Judge Peck cites studies that the contents of the "seed set" are much less significant with tools using "continuous active learning" in which the model is continually trained as reviewers review all documents identified as potentially relevant. *See id.*, 306 F.R.D. at 127.

Fourth, and most significantly, Judge Peck points out that there are alternatives to sharing coding decisions on the training set to insure the defensibility of a predictive coding protocol. "[R]equesting parties can insure that training and review was done appropriately by other means, such as statistical estimation of recall at the conclusion of the review as well as by whether there are gaps in the

production, and quality control review of samples from the documents categorized as non-responsive." *See id.*, 306 F.R.D. at 128-29. *See also* Gareth Evans and David Grant, *Metrics that Matter: Van Halen, M&Ms and Metrics in E-Discovery* (2015 White Paper).

Judge Peck, of course, recognizes that it should be up to the responding party to decide what search and review methodology to use and that, as before, the developments since *Da Silva Moore* do "not mean [predictive coding] must be used in all cases." *See id.* at 126 (quoting *Da Silva Moore*, 287 F.R.D. at 193). Indeed, he points out that "[i]n contrast, where the requesting party has sought to force the producing party to use TAR, the courts have refused." *Id.*, 306 F.R.D. at 127 n.1 (listing cases).

There were other decisions involving predictive coding during the first half of 2015. The District of Connecticut approved an ESI stipulation that explicitly provided that a responding party "need not share the intricacies of [its production] methodology unless and until there is a good faith allegation of a violation of Rule 26." Thus, if a party opted to use predictive coding it need only "disclose its intent to use that technology and the name of the review tool." *Connecticut Gen. Life Ins. Co. v. Health Diagnostic Lab., Inc.*, No. 3:14-cv-01519, 2015 WL 417120 (D. Conn. Jan. 28, 2015).

The District of Nebraska recognized that "[p]redictive coding is now promoted (and gaining acceptance) as not only a more efficient and cost effective method of ESI review, but a more accurate one." *Malone v. Kantner Ingredients, Inc.*, No. 4:12-cv-3190, 2015 WL 1470334, at *3 n.7 (D. Neb. Mar. 31, 2015).

In *Chevron Corp. v. Snaider*, No. 14-cv-01354-RBJ-KMT, 2015 WL 226110 (D. Col. Jan. 15, 2015), the district court refused to quash a subpoena seeking discovery into an international racketeering scheme, rejecting the resisting party's undue burden objections in part because "Snaider does not address the likelihood that in a case such as this computer-assisted review would no doubt be invoked, and while that is costly, it is much more efficient than assigning individuals to review a large volume of paperwork." *Id.* at *11, n.9.

Thus, in the first half of 2015, more courts have referred to predictive coding as a viable option for document search and review, and Judge Andrew Peck in his *Rio Tinto* decision has helped develop a more well thought-out predictive coding jurisprudence, the need for which we lamented in our 2014 Year-End E-Discovery Update.

Back to Top

Sanctions

Many of the sanctions cases in 2015 have grappled more with the type of conduct that justifies imposition of sanctions, rather than the question of what type of sanctions are appropriate. Continuing a trend that we have seen in recent years, sanctions were imposed not only for spoliation--*i.e.*, failing to preserve relevant information after a duty to preserve arose--but also for delayed production of relevant and responsive information.

Failure to Preserve

The first half of 2015 has already seen several important sanctions decisions dealing with spoliation. As usual, these decisions echo a persistent theme: the importance of implementing a timely and effective litigation hold.

In *Clear-View Technologies*, 2015 WL 2251005, Magistrate Judge Paul Grewal of the Northern District of California found defendants had an obligation to preserve evidence once the plaintiff's CEO sent them text messages threatening a lawsuit, which occurred a full two years before the suit was filed. *See id*. at *7. After receiving these text messages, Defendants intentionally deleted relevant documents, failed to implement a hold or monitoring policy, and ran a "Crap Cleaner" software to wipe files on a laptop while plaintiffs' motion to compel was pending. *See id*. at *1, *7.

As is often the case in sanctions cases, bad facts invite the court to make an example of defendants, and here the court imposed severe sanctions for spoliation of evidence--a joint monetary sanction of $212,320 against defendants and defense counsel and an adverse jury instruction. *See id.* at *8 & n. 90. While this case garnered attention for the harshness of the sanctions, its most important takeaway is that courts may find that informal communications, such as text messages, may be sufficient to trigger the duty to preserve evidence. Indeed, the court made clear that, in its view, there was no doubt that defendants were on notice of foreseeable litigation in this case--"[t]his call is not even close." *Id*. at *7.

In *Fidelity Nat. Title Ins. Co. v. Captiva Lake Inv., LLC*, No. 4:10-CV-1890, 2015 WL 94560 (E.D. Mo. Jan. 7, 2015), the court imposed sanctions on a plaintiff whose failure to institute a litigation hold resulted in the mass deletion of relevant emails. Following a protracted dispute between the parties regarding the adequacy of plaintiff's production of ESI, the court granted defendant's request for a specialist to examine plaintiff's computer systems. The specialist found, among other things, that plaintiff (1) had not instituted a litigation hold, (2) did not conduct a systematic search of its computer systems for discoverable information, (3) and allowed a contractor to delete as many as 13 million emails after the commencement of litigation. *See id*. at *2.

The court found that the email deletions likely caused the loss of discoverable emails and that the defendant was prejudiced by the loss of these emails. *See id.* at *3. Significantly, the court held that the plaintiff's "failure to implement a litigation hold . . . establishes the necessary intent to support the imposition of sanctions." *Id.* Based on these findings, the court issued an adverse inference instruction with respect to the deleted emails and ordered plaintiff to pay fees and expenses related to the delay caused by its "mishandling of discovery." *Id*. at *7.

In a rare appellate decision on spoliation, *Blue Sky Travel & Tours, LLC v. Al Tayyar*, No. 13-2500, 2015 WL 1451636 (4th Cir. Mar. 31, 2015), the Fourth Circuit vacated sanctions for spoliation imposed by a lower court after finding the lower court applied the incorrect standard when assessing a defendant's duty to preserve evidence. The Fourth Circuit took the opportunity to clarify both the scope of a litigant's duty to preserve and the purpose of a litigation hold.

In the underlying trial court case, Defendant ATG repeatedly failed to produce copies of certain original invoices that it was ordered to turn over by the magistrate judge. ATG claimed it did not have

these invoices because its document retention practice was to discard the original invoices after transcribing the information contained in these invoices into a Microsoft Excel spreadsheet. *See id*. at *3. The magistrate judge rejected this argument and held that once litigation commenced, ATG had an obligation to discontinue its document retention policies and preserve "*all documents*." *Id*. at *8 (emphasis in original). Finding ATG liable for spoliation, the magistrate judge issued an adverse jury instruction, which "effectively relieved [plaintiff] of its burden to prove its damages claim for lost profits." *Id*.

The magistrate judge's rulings were upheld by the district court. On appeal, however, the Fourth Circuit found that the magistrate judge and district court had applied the incorrect standard to ATG's duty to preserve evidence, stating "a party is *not required to preserve all its documents* but rather only documents that the party knew or should have known were, or could be, relevant to the parties' dispute." *Id*. at *8 (emphasis added).

A final noteworthy recent decision is *Malibu Media, LLC v. Tashiro*, No. 1:13-CV-00205, 2015 WL 2371597 (S.D. Ind. May 18, 2015), which presents a thorough analysis regarding whether a court may issue a sanction for spoliation of evidence where a party intentionally deletes electronic files that may be subsequently recovered. Plaintiff brought suit against defendants, a married couple, alleging they had used a BitTorrent client to illegally download and distribute plaintiff's copyrighted works. During discovery, defendants agreed to produce their hard drives for forensic analysis. Plaintiff's expert determined that a large number of files were permanently deleted from the hard drives the very night before the hard drives were produced. *See id*. at *1-*2. Defendants' expert agreed that files were deleted from the hard drives but claimed that he was able to recover all of the deleted files. *See id.* at *2.

Plaintiff contended defendants had destroyed evidence by deleting the files that would have exposed them to liability. *See id*. at *17. Defendants countered that no spoliation had occurred because all the deleted files were recoverable and plaintiff was thus not prejudiced by the "deletions." *See id*. at *18. The magistrate judge sided with plaintiff, finding defendants liable for spoliation because it was "highly likely" that the files were deleted *and* unrecoverable, *id*. at *19, and because defendants had deleted these files in bad faith, *see id.* at*13-*19.

Significantly, the magistrate judge went on to explain that even if the deleted files were recoverable, defendants would not have been absolved of liability for spoliation. *See id*. at *19. As a practical matter, the magistrate judge noted that the "mere deletion of files has evidentiary ramifications" as it can alter the metadata associated with those files. *Id*. at *21. But more importantly, the magistrate judge rejected defendants' assertion that a permanent loss of evidence is a prerequisite to a finding of spoliation. *See id.* at *19. To the contrary, the magistrate judge stated that "the Seventh Circuit has implicitly acknowledged that recovery of deleted or destroyed evidence does not preclude entry of sanctions." *Id.* at *21 (citing *Barnhill v. United States*, 11 F.3d 1360, 1367-68 (7th Cir. 1993)).

According to the magistrate judge, the recoverability of the files would not change the fact that defendants "attempted to work a fraud on this Court, obstruct Plaintiff's pursuit of its case, and subvert the judicial process." *Id*. Accordingly, "even if [defendants'] conduct had not harmed Plaintiff, the

Court would not allow [their] attempted fraud to go unpunished." *Id*. In the end, the magistrate judge imposed the most severe sanction against defendants--an entry of default judgment--because in addition to spoiling evidence, the defendants had committed perjury by making false representations regarding the evidence during their depositions. *See id*. at *37-*38.

Significantly, it appears that this decision may have come out very differently if the pending amendment to Federal Rule of Civil Procedure 37(e) had been in effect, as it forecloses the imposition of sanctions if the deleted information can be recovered or obtained from other sources.

Failure to Produce

As we have increasingly seen in recent years, courts in the first half of 2015 addressed whether sanctions should be imposed because of delayed productions.

In *Oracle Am., Inc. v. Terix Computer Co., Inc.*, No. 5:13-CV-03385, 2015 WL 2398993 (N.D. Cal. May 19, 2015) (Grewal, Mag.), plaintiffs learned of the existence of a laptop containing relevant information during a deposition of one defendant's employee at the close of fact discovery. *See id*. at *2-*3. Although defendants later produced the laptop, plaintiffs moved for sanctions, alleging defendants intentionally withheld the laptop. *See id.* at *3. The magistrate judge declined to impose sanctions after finding there was insufficient evidence that defendants had acted in bad faith. *Id.* at *4. Specifically, plaintiffs failed to show that defendants intentionally misrepresented the existence of this laptop. *Id*. "[W]ithout clear evidence of bad faith," the magistrate judge noted, it would be inappropriate to sanction defendants for their initial failure to produce the laptop. *Id*.

Likewise, in *Logtale, Ltd. v. IKOR, Inc.*, No. C-11-5452, 2015 WL 581513 (N.D. Cal. Feb. 11, 2015) (Ryu, Mag.), the court considered the appropriate sanctions for defendant's repeated failures to produce responsive documents in accordance with court-ordered deadlines. *See id.* at *3. Because plaintiffs failed to offer "any argument or evidence" with respect to defendant's willfulness, fault, or bad faith, the magistrate judge declined to impose a terminating sanction. *See id.* at *3-4. However, the magistrate judge ordered defendants to pay for plaintiff's reasonable expenses caused by their failure to comply with discovery orders. *Id*. at *4.

Finally, in *Parsi v. Daioleslam*, 778 F.3d 116 (D.C. Cir. 2015), the D.C. Circuit reaffirmed that a district court seeking to impose monetary sanctions under its inherent judicial authority--as opposed to its authority pursuant to Rule 37--must first find by clear and convincing evidence that the party committing the improper conduct acted in bad faith. In the case, plaintiffs repeatedly failed to produce relevant documents, including highly relevant emails between plaintiffs and third parties. *Id.* at 124.

On top of sanctions it imposed for violations of its discovery orders, the court exercised its inherent authority to order plaintiffs to pay attorney's fees and expenses specifically related to its failure to produce the emails. *Id*. at 119-120. The D.C. Circuit determined that the imposition of this particular sanction required a finding of bad faith conduct under a clear and convincing standard of proof. It then held that the district court met this obligation, as it had provided ample support on the record for its conclusion that plaintiffs' failures to produce these emails were "indefensible" and "inexplicable." *Id.* at 132. If the pending amendment to Federal Rule of Civil Procedure 37(e) becomes effective on

December 1, 2015, we will not likely see future sanctions decisions resting on the court's inherent authority, as the Advisory Committee Note to the amendment declares that the amended rule precludes the issuance of sanctions based on courts' inherent authority.

Finally, one court found during the first half of 2015 that failure to provide documents in an accessible format can be sanctionable. In *Boxer F2, L.P. v. Flamingo W., Ltd.*, No. 14-CV-00317, 2015 WL 2106101 (D. Colo. May 4, 2015) (Watanabe, Mag.), the court granted plaintiff's renewed request for sanctions for generally obstructive discovery conduct. In an "effort to reduce further gamesmanship over the precise wording or scope of Plaintiff's discovery requests," the magistrate judge previously ordered defendants to produce complete copies of certain accounting records. *Id.* at *1. Defendants provided plaintiff with the records via a Dropbox hyperlink, but did not provide plaintiff a functioning username or password until almost a month later. *Id.*

The court found defendants did not give plaintiff "any meaningful access" to the accounting records, *id.* at *3, and it further found that defendants had modified the records prior to production, *see id*. Because defendants failed to comply in good faith with discovery orders, the magistrate judge ordered defendants to pay fees and expenses related to plaintiff's renewed motion for sanctions and entered certain factual allegations in plaintiff's complaint as findings of fact for the purposes of the litigation. *Id*. at *4.

Back to Top

Preservation

Courts issued several interesting decisions in the first half of 2015 regarding (1) the trigger of the duty to preserve, (2) the extent to which the duty reaches data in the possession of non-parties, and (3) the subject matter breadth of the duty.

Many who are not immersed in e-discovery are surprised to learn that the duty to preserve documents and ESI that are relevant to the litigation can be triggered before suit is filed--in some cases long before. In the Seventh Circuit, the duty to preserve is only triggered when a litigant knew or should have known that litigation was imminent. In all other Circuits, however, courts expect a greater deal of clairvoyance, holding that the duty to preserve begins when litigation is "reasonably foreseeable."

In *Clear-View Technologies*, 2015 WL 2251005, Magistrate Judge Paul Grewal of the Northern District of California ruled that the duty to preserve arose over two years before the plaintiff commenced its lawsuit. The case involved less than model behavior on the part of the defendants--after receiving a legal hold notice from the plaintiff "in anticipation of litigation," they nevertheless failed to take any active steps to preserve data, deleted relevant text messages, and they lost and threw away several iPhones and other devices with unique relevant information. Additionally, after being served with document requests in the litigation, they failed to take reasonable steps to search for responsive documents, and one defendant deployed "Crap Cleaner" and other wiping software to remove data from his laptop computer while a motion to compel was pending. *See id.* at *1-5.

Finding the duty to preserve to have attached upon defendants' receipt of the legal hold notice would have been less controversial. The court, however, found that it arose approximately six months earlier, when the plaintiff's CEO sent the defendants angry text messages saying "don't call my shareholders with your b.s. . . . [K]eep it up and you'll find [yourself] in court. Call Clyde again and I sue." The next morning, however, he sent apologetic texts, and acknowledged that he had been drinking ("I was very upset last night, plus the booze"). The court nevertheless noted that plaintiff's CEO did not retract the threat of suit. *Id.* at *2, *7. Combined with defendants' discussion among themselves about the potential legal ramifications of their conduct later the same month, the court found that "[t]his call is not even close" under the reasonable foreseeability standard. *See id.* at *7.

The extent to which a duty to preserve extends to documents in the possession of non-parties is usually determined by whether they are deemed to be under the control of a party. Three decisions in the first half of 2015 addressed whether parties had such control.

In *Wandering Dago Inc. v. N.Y. State Office of Gen. Servs.*, No. 1:13-CV-1053, 2015 WL 3453321, at *11 (N.D.N.Y. May 29, 2015) (Treece, Mag. J.), the court addressed whether a New York state agency was obligated to preserve emails from a nonparty witness in a separate state agency. *Id.* at *7. The court found that "state agencies for most purposes are separate and distinct organs and should not be viewed in the aggregate," and that "[c]onsidering that hundreds of lawsuits are filed daily against New York State . . . requiring each agency and thousands of officials to institute a litigation hold every time a party contemplates or even commences litigation against another agency would paralyze the State." *Id.* at *8.

In *Superior Performers, Inc. v. Meaike*, No. 1:13CV1149, 2015 WL 471429, at *3 (M.D. N.C. Feb. 4, 2015), the court found that the plaintiffs had "control" over voicemail that was not stored on their phones. The court held that "even if a party does not physically control the evidence, the party still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence." *Id.* (internal quotations omitted).

Further considering the limitations of control, the court in *Perez v. Metro Dairy Corp.*, No. 13 CV 2109, 2015 WL 1535296, at *1 (E.D.N.Y. Apr. 6, 2015) (Levy, Mag. J.) addressed whether a party had control over records that had been seized pursuant to an order in another matter and therefore were no longer in its possession. Noting that defendants had stated that the records had been seized within 24 hours of the order with no opportunity to back them up, the court found no obligation to have done so. *Id.* at *3.

Finally, a Circuit Court confirmed that the scope of the duty to preserve is limited to documents relevant to the dispute, and a party cannot be required to preserve all documents in its possession, custody or control. In *Blue Sky Travel & Tours*, 2015 WL 1451636, at *8, the Fourth Circuit held that it was an abuse of discretion for the magistrate judge to have concluded that a party "had a duty to stop its document retention policies and to preserve *all documents* because you don't know what may or may not be relevant." (emphasis in original) (internal quotation marks omitted). Instead, according to

the court, "a party is not required to preserve all its documents but rather only documents that the party knew or should have known were, or could be, relevant to the parties' dispute." *Id.* (citations omitted).

Back to Top

E-Discovery Cost Recovery

Parties increasingly are seeking to recover a portion of their e-discovery costs pursuant to 28 U.S.C. § 1920(4), which permits the taxing of "[f]ees for exemplification and the costs of making copies of any materials where the copies are necessarily obtained for use in the case." The first half of 2015 was no exception.

Although the reference in 28 U.S.C. § 1920(4) to the recovery of the costs of making "copies" is somewhat anachronistic in the digital age, courts have nonetheless applied § 1920(4) to e-discovery by way of analogy, with the issue often being what qualifies as a "copy." *See Fitbug Ltd. v. Fitbit, Inc.*, No. 13-1418 SC, 2015 WL 2251257, at *3-4 (N.D. Cal. May 13, 2015) (discussing how a vacuum of case law interpreting § 1920(4) required courts to use analogies and that e-discovery costs were necessarily incurred in complying with the parties' production agreement).

In *Colosi v. Jones Lang LaSalle Americas, Inc.*, 781 F.3d 293, 297 (6th Cir. 2015), the Sixth Circuit explained, "[i]maging a hard drive falls squarely within the definition of 'copy'" and affirmed the judgment of costs in favor of a defendant employer in a wrongful termination suit. The plaintiff--in response to a court order compelling production--delivered her computer to her attorney's office and demanded that defendant employer send a third-party vendor to image it. *See id.* at 298. Imaging the computer was the "sole avenue permitting review of [the plaintiff's] files" and was analogous to the taxable "cost of a party delivering an image file in response to an opponent's production request." *See id.*

The *Colosi* court expressly distinguished *Race Tires America, Inc. v. Hoosier Racing Tire Corp.*, 674 F.3d 158, 166-72 (3d Cir. 2012)--upon which the plaintiff relied in opposing the bill of costs--saying *Race Tires* was "overly restrictive" because it excluded all e-discovery expenses except those associated with converting responsive documents to an agreed upon format. *See Colosi*, 781 F.3d at 297.

Likewise, in *Resnick v. Netflix, Inc. (In re Online DVD-Rental Antitrust Litig.)*, 779 F.3d 914, 928 (9th Cir. 2015), the Ninth Circuit affirmed the trial court's award of e-discovery costs, including not only those costs attributable to OCR and converting documents to TIFF (*see id.* at 932). The court remanded claims for other categories of e-discovery costs because the requesting party's description of those tasks was not sufficiently detailed. *See id.* at 930-31.

Although *Colosi* and *Resnick* signal an increasing openness of the judiciary to taxing e-discovery costs, and *Colosi* rejected *Race Tires* as "overly restrictive", several courts nonetheless continue to rely upon *Race Tires* and follow its narrow interpretation of § 1920(4). *See e.g., CSP Techs., Inc. v. Sud-Chemie AG*, No. 4:11-cv-00029-RLY-WGH, 2015 WL 2405528, at *3-4 (S.D. Ind. May 20, 2015); *Comprehensive Addiction Treatment Ctr., Inc. v. Leslea*, No. 11-cv-03417-CMA-MJW, 2015 WL

638198, at *2 (D. Colo. Feb. 13, 2015); *see also Bagwe v. Sedgwick Claims Mgmt. Servs., Inc.*, No. 1:11-cv-02450, 2015 WL 351244, at *5-6 (N.D. Ill. Jan. 27, 2015) (Mag. J. Young Kim).

Parties and courts are also taking a more proactive, forward-looking approach to shifting e-discovery costs, raising the issue of who should pay for e-discovery before they even incur the costs. For example, in *United States ex rel. Carter v. Bridgepoint Education, Inc.*, 305 F.R.D. 225, 247 (S.D. Cal. 2015), plaintiffs requested backup tapes that defendants argued were inaccessible because of the burden and cost in producing the tapes. Magistrate Judge William Gallo said that "[t]o obtain this ESI at the other's expense, the requesting party must demonstrate need and relevance that outweigh the costs and burdens of retrieving and processing this provably inaccessible information." *Id.* at 239.

After determining the backup tapes were minimally relevant and inaccessible--they were inaccessible because of the defendants' established data retention scheme--he ordered plaintiffs to bear the cost of recovery and search, and defendants to bear the cost of production. *See id.* at 240-44. As Judge Gallo implicitly recognized, shifting costs before they are even incurred can encourage the parties to be more reasonable about the scope of discovery they seek.

Back to Top

Discovery of Social Media

Reflecting that the use of social media continues to proliferate in business and social contexts, the number of cases focusing on the discovery of social media continued to skyrocket in the first half of 2015. Courts are still struggling to develop rules and protocols applicable to social media evidence, including whether special authentication rules should govern social media evidence, what threshold showing of relevance must be made before discovery of personal social media data should be allowed, when the duty to preserve social media evidence arises, what role privacy rights should play in social media discovery, and who should bear the burden of reviewing social media data.

The first half of 2015 included a major shift in the law governing the authentication of social media evidence. The Court of Appeals of Maryland changed course, and "embrace[d]" the Second Circuit's holding that "in order to authenticate evidence derived from a social networking website, the trial judge must determine that there is proof from which a reasonable juror could find that the evidence is what the proponent claims it to be." *Sublet v. State*, 113 A.3d 695, 698, 718, 722 (Md. 2015) (citing *U.S. v. Vayner*, 769 F.3d 125 (2d Cir. 2014)). Previously in Maryland, social media evidence was admissible only if the judge was "convince[d] . . . that the social media post was not falsified or created by another user." *Griffin v. State*, 19 A.3d 415 (Md. 2011).

Under *Sublet*, the preliminary determination of authentication is made by the trial judge and is a "context–specific determination" based on proof that "may be direct or circumstantial." *Id.* at 715 (citing *Vayner*). The court noted that "[t]he standard articulated in *Vayner* … is utilized by other federal and State courts addressing authenticity of social media communications and postings" and "is not particularly high." *Id.* at 715, 718 (citations and internal quotations omitted). The court's decision in *Sublet* could very well signal the death knell of a trend wherein some courts required "'greater scrutiny' or particularized methods for the authentication of evidence derived from the Internet due to a

'heightened possibility for manipulation,'" (*Vayner*, 769 F.3d at 131 n.5 (citing *Griffin*)), as *Griffin* was the most influential of such cases.

In addition, in the first half of 2015, courts continued to find that the testimony of the individual who printed a copy of a social media webpage, or prepared a memorandum summarizing information obtained from the social media account, is insufficient to authenticate social media evidence. *See, e.g., Linscheid v. Natus Medical Inc.*, No. 3:12-cv-76-TCB, 2015 WL 1470122, at *5-6 (N.D. Ga. Mar. 30, 2015) (finding Linkedin profile page not authenticated by declaration from individual who printed the page from the Internet); *Monet v. Bank of America, N.A.,* No. H039832, 2015 WL 1775219, at *8 (Cal Ct. App. Apr. 16, 2015) (finding that a "memorandum by an unnamed person about representations others made on Facebook is at least double hearsay" and not authenticated).

Courts also continue to hold that "the fact that the information [sought] is in an electronic file as opposed to a file cabinet does not give [the party seeking discovery] the right to rummage through the entire file." *Silva v. Dick's Sporting Goods, Inc.*, No. 3:14cv580 (WWE)(WIG), 2015 WL 1275840, at *1-2 (D. Conn. Mar. 19, 2015) (Garfinkel, Mag. J.) (refusing defendant's request for copies of all of plaintiff's Facebook communications, many of which plaintiff argued were not relevant to the claims and defenses involved in the dispute) (citations and quotations omitted); *see also Cummings v. Bost, Inc.*, No. 2:14–CV–02090, 2015 WL 1470137, at *9 (W.D. Ark. Mar. 31, 2015) (refusing defendant's request for access to plaintiff's Facebook account because the request was "rooted in pure speculation").

As with more traditional forms of evidence, the party seeking discovery of social media "must establish a factual predicate for [the] request by identifying relevant information in [the social media] account, such as information that contradicts or conflicts with plaintiff's alleged [claims]." *Gonzalez v. City of New York*, 47 Misc. 3d 1220(A), 2015 WL 2191363, at *1 (N.Y. Sup. May 4, 2015) (citations and quotations omitted). One court took a novel approach to the establishment of a factual predicate, ordering plaintiff to produce a sample of plaintiff's Facebook activity limited to specific references to plaintiff's emotional distress claims and any related treatment. *Caputi v. Topper Realty Corp.*, No. 14–cv–2634(JFB)(SIL), 2015 WL 893663, at *8 (E.D.N.Y. Feb. 25, 2015). The court held that the defendants could review this sample and use it to put forth a factual predicate to obtain additional discovery from plaintiff's Facebook account information. *Id.*

Once a factual predicate has been established, as with other forms of evidence, most courts only grant discovery of social media evidence that is relevant to the issues involved in the case. In *Gonzalez*, defendant demonstrated that photographs and comments posted by plaintiff regarding his injuries and the accident in question established that "discovery of plaintiff's social media account will lead, or may reasonably be calculated to lead, to relevant evidence bearing on plaintiff's claims." 2015 WL 2191363 at *2. Accordingly, the court ordered discovery of materials on plaintiff's social media accounts relevant to plaintiff's claims and injuries, but denied defendant's request to access any other social media information. *Id. See also In re Milo's Kitchen Dog Treats Consol. Cases*, No. 12–1011, 2015 WL 1650963, at *1-5 (W.D. Pa. Apr. 14, 2015) (refusing defendant's request for "unfettered access to [p]laintiff's Facebook data" where plaintiff had already provided relevant information from

Facebook account); *Spearin v. Linmar, L.P.*, 2015 WL 3678163 at *1 (N.Y. App. Div. June 16, 2015) (granting discovery of social media evidence relevant to alleged injuries only).

Another continuing theme in the first half of 2015 was the extent to which parties have an obligation to preserve social media during litigation, and whether the modification of social media constitutes sanctionable spoliation. Because social media is dynamic, account holders may delete information from their page or cancel their account altogether, without realizing that the information could be relevant to an anticipated or pending matter. In addition, information can be deleted from a post by other users who do not have a duty to preserve evidence.

In determining whether to award sanctions for spoliation of social media, courts have focused on a variety of factors, including whether the users had a duty to preserve their account at the time the evidence was deleted, and whether the users deleted the social media data to hide adverse evidence.

In *D.O.H. v. Lake Central School Corp.*, plaintiff admitted to deleting some relevant information from his Facebook account prior to the court order requiring preservation of evidence, and admitted that he may also have deleted some posts after the order was issued. No. 2:11–cv–430, 2015 WL 736419, at *8-10 (N.D. Ind. Feb. 20, 2015) (Rodovich, Mag. J.) (considering spoliation sanctions for deletion of posts and comments from Facebook). The court found that plaintiff had a duty to preserve evidence starting when he knew litigation was imminent, and thus the evidence was spoliated. *Id.* at *10. The court held, however, that an adverse inference sanction was not warranted, as plaintiff did not delete the information in bad faith to hide adverse evidence. *Id.* The court noted that it was likely plaintiff deleted some "vulgar comments to avoid embarrassment or further harassment," and that it was possible third party users, not plaintiff, had deleted their own comments on plaintiff's Facebook page. *Id.*

A frequently litigated issue regarding the discovery of social media is the role of traditional privacy rights in protecting those new methods of personal expression. In the first half of 2015, most courts continued to find that individuals generally do not have a reasonable expectation of privacy, regardless of activated privacy settings, in the information they submit to social networking sites. *See Nucci v. Target Corp.*, 162 So.3d 146, 153-55 (Fla. Dist. Ct. App. Jan. 7, 2015) (finding no reasonable expectation of privacy in social media accounts because "[b]y creating a Facebook account, a user acknowledges that her personal information would be shared with others. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist.") (internal citations and quotations omitted); *In re Milo's Kitchen*, 2015 WL 1650963, at *3 (holding "there is no reasonable expectation of privacy in information posted on Facebook and … making a Facebook page 'private' does not shield it from discovery if the information sought is relevant").

At least one court found, however, that there is "a reasonable expectation of privacy attached to the one-on-one messaging option that is available through Facebook accounts" and thus granted discovery of plaintiff's Facebook postings, comments, videos, and photographs, but not private messages sent or received by plaintiff. *Melissa G v. North Babylon Union Free School Dist.*, 6 N.Y.S.3d 445, 449 (N.Y. Sup. Ct. 2015); *see also Cummings*, 2015 WL 1470137, at *9 (refusing defendant's request for access

to plaintiff's Facebook account in part because it "would allow a substantial intrusion into [plaintiff's] privacy for which [defendant] has failed to provide a sufficient justification").

The question of who should bear the burden of review has become more important as the volume and costs of electronic discovery increase. In the first half of 2015, most courts continued to require the account holder to gather and review data from social networking accounts, and provide it directly to the defendant, as typically "counsel for the producing party is the judge of relevance in the first instance" for discovery matters. *Melissa G*, 6 N.Y.S.3d at 447-49 (ordering plaintiff's counsel to review plaintiff's Facebook postings and produce those relevant to plaintiff's damages claim, as "there [was] no basis to believe that plaintiff's counsel [could not] honestly and accurately perform the review function") (internal citations omitted).

A small minority of courts, however, conduct an *in camera* review of the social media content being sought. Some courts have chosen this method of review to resolve disputes regarding whether certain communications on social media accounts are privileged. *See, e.g., In re Milo's Kitchen*, 2015 WL 1650963, at *1-5 (ordering plaintiff to produce social media evidence for *in camera* inspection so the court could review for privilege). Other courts have chosen *in camera* review for social media data because social media accounts "may contain material of a private nature that is not relevant." *Gonzalez*, 2015 WL 2191363, at *1-2 (holding that "the Supreme Court should conduct an *in camera* inspection of all status reports, e-mails, photographs, and videos posted on the plaintiff's social media accounts since the date of the accident to determine which of those materials, if any, are relevant to the alleged claim and injuries"); *see also Spearin*, 2015 WL 3678163 at *1 (overturning lower court's order requiring plaintiff to provide defendant access to his entire Facebook account, and remanding for an *in camera* review of plaintiff's Facebook account instead).

By contrast, other courts have acknowledged that social media accounts could contain "embarrassing" content, but have allowed its discovery and refused to preclude it from evidence, reserving the discretion to later exclude the evidence at trial pursuant to Federal Rule of Evidence 611, which allows a court to control the examination of witnesses and presentation of evidence to protect witnesses from harassment and undue embarrassment. *See Newill v. Campbell Transp. Co.,* Inc., 2015 WL 267879, *1-2 (W.D. Pa. Jan. 14, 2015) (refusing to preclude the defendant from introducing several of the plaintiff's Facebook postings into evidence because they were embarrassing to plaintiff).

Back to Top

Government Investigations

Courts continue to grapple with how to apply e-discovery concepts to governmental investigations. In a number of decisions during the first half of 2015, courts have sought to balance Fourth Amendment rights with the opportunities for discovery created by the Stored Communications Act (SCA), 18 U.S.C. §§ 2700 *et. seq,*, which permits access to the files of technological intermediaries, such as Internet service providers and cell phone providers.

Notably, in the first half of 2015, the Eleventh Circuit joined several other courts in holding that the Government's receipt of a robbery suspect's historical cell tower records pursuant to the SCA does not

violate a defendant's Fourth Amendment rights, even if the information is obtained without a search warrant and its requisite showing of probable cause, as long as the Government complies with the SCA. *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015). *See also, e.g., In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013) (holding in a 2-1 opinion that historical cell site records under the SCA did not "categorically" violate the Fourth Amendment); *In re United States For An Order Directing Provider Of Electronic Communication Service To Disclose Records*, 620 F.3d 304 (3d Cir. 2010) (approving constitutionality of § 2703(d)); *United States v. Epstein*, CR No. 14-287 (FLW), 2015 WL 1646838 (D.N.J. Apr. 14, 2015); *United States v. Dorsey*, No. CR 14-328-CAS, 2015 WL 847395, at *6-8 (C.D. Cal. Feb. 23, 2015); *United States v. Lang*, No. 14 CR 390, 2015 WL 327338, at *3-4 (N.D. Ill. Jan. 23, 2015) (collecting cases); *United States v. Shah*, No. 5:13-cr-328-FL, 2015 WL 72118 (E.D. N.Ca. Jan. 6, 2015) (holding that there is no Fourth Amendment right to protection against government's access of cell phone location data from cell company or of user's IP addresses used to access Facebook); *but see United States v. Cooper*, No. 13-cr-00693, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015) (coming to the opposite conclusion with respect to historical cell tower record information).

Considering the Supreme Court's decisions in *United States v. Miller*, 425 U.S. 435, 437-38 (1976), where the Court held that the defendant had no Fourth Amendment interest in his bank account records because they were also the bank's business records, the Eleventh Circuit reasoned in *Davis* that the defendant did not own or possess the mobile phone company's business records. *Davis*, 785 F.3d at 511. "Instead those cell tower records were created by Metro PCS, stored on its own premises, and subject to its control. Cell tower locations do not contain private communications of the subscriber. This type of *non-content evidence*, lawfully created by a third-party telephone company for legitimate business purposes, does not belong to [the defendant], even if it concerns him." *Id.*

In addition, the Eleventh Circuit considered the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735, 742-46 (1979), where the Court held that telephone users have no reasonable expectations of privacy in dialed telephone numbers recorded through pen registers and contained in the third-party telephone company's records. Similar to *Smith*, the Eleventh Circuit concluded the defendant had no "subjective or objective reasonable expectation of privacy in MetroPCS's business records showing the cell tower locations that wirelessly connected his calls at or near the time of the ... robberies." *Id.*

At least some courts have taken the same approach to governmental tracking and monitoring of an individual's cell phone data. The Northern District of Mississippi held that there is no reasonable expectation of privacy in *prospective* cell phone tower data (*i.e.*, where permission to collect the data is sought prospectively, rather than after the fact), and the court held that the government could actively track and monitor cell phone data. *In re the Application of the U.S. for an Order for Authorization to Obtain Location Data Concerning an AT&T Cellular Telephone*, --- F. Supp. 3d ----, No. 3:15MC3, 2015 WL 184276, at *5-6 (N.D. Miss. Mar. 30, 2015) (reviewing cases and holding that in light of the "clearly binding Fifth Circuit precedent" that "there is no reasonable expectation of privacy in historical cell phone data," there is similarly no reasonable expectation of privacy in prospective cell phone data as the court "doubt[ed] that prospective cell phone data [was] sufficiently different from historical cell phone data to warrant a different result").

But this decision appears to be at odds with a number of other courts, which have required the government to show probable cause to track and monitor cell phone usage of a suspect. *See, e.g.*, *United States v. Cooper*, No. 13-cr-00693-SI-1, 2015 WL 881578, at *4-5 (N.D. Cal. Mar. 2, 2015) (collecting cases); *Dorsey*, 2015 WL 847395, at *9 (citing *United States v. Espudo*, 954 F. 3d 1029, 1035 (S.D. Cal. 2013) (collecting cases)) (finding that "a majority of courts have taken the position that the government must make a showing of probable cause to acquire 'real-time' or 'prospective' cell site location data")..

Courts have also permitted the government to expansively use the SCA to apprehend suspects, rather than simply to gather evidence. For example , in *In the Matter of Application for Cell Tower Records under 18 U.S.C. § 2703(D)*, --- F. Supp. 3d ----, No. H-15-136M, 2015 WL 1022018 (S.D. Tex. Mar. 9, 2015), the Southern District of Texas issued an order under the SCA for a literal "dump" of cell phone record information from seven different cell phone service providers, which the government had requested in order to "identify the particular device used by the suspect and any confederates, and ultimately to enable their capture and arrest." The Government filed an application under § 2703(d) of the SCA for "an order compelling seven different cell phone service providers to release historical cell tower data for specific towers providing service to a crime scene within Houston city limits at the hour of the crime." *Id.* at *1. As the Court put it, the request was "unusual" because unlike most account record requests under the SCA, the "targeted account [was] not specified." *Id*.

Keeping with this expansive approach in the context of governmental investigations, a court in the Eastern District of New York concurred with the holdings of other courts in other districts that, pursuant to the SCA, a judge may issue a warrant for the production of email evidence stored in a district other than the one in which he or she sits. *United States v. Scully*, No. 14-CR-208(ADS), --- F.3d ---- (E.D.N.Y. June 8, 2015); *see also, e.g., United States v. Berkos*, 543 F. 3d 392 (7th Cir. 2008) (holding that § 2703(a) permits the issuance of warrants for electronic evidence stored outside of the issuing district); *United States v. Kernell*, No. 3:08-CR-142 (CCS), 2010 WL 1408437 (E.D. Tenn. Apr. 2, 2010), *report and recommendation adopted*, No. 3:08-CR-142 (TWP), 2010 WL 1491831 (E.D. Tenn. Apr. 13, 2010) (same); *United States v. Noyes*, No. 1:08-CR-55 (SJC), 2010 WL 5139859, at *9 n.8 (W.D. Pa. Dec. 8, 2010) (same).

In *Scully*, the defendant filed a motion to suppress email evidence produced by Yahoo pursuant to a search warrant issued by Judge Wall in the Eastern District of New York, arguing that the search warrant violated Federal Rule of Criminal Procedure 41 and § 2703 of the SCA because the emails were stored in California and "a judge in one district cannot issue a search warrant for property located in another district." *Id.* at *11. After an extensive examination of the relevant rules, statutes, legislative history, and precedent, the Court in *Scully* held that the search warrants did not violate the Rule 41 or the SCA, and that a court in one district may issue a search warrant for electronically stored information stored in another district. *Id.* at *20.

One limitation that courts seem to put on government investigations into files maintained by ISPs and other similar intermediaries is that courts are reluctant to burden the intermediaries with the obligation to sift through voluminous information and identify the responsive/relevant data. In one example, the District of Alaska determined that requiring an ISP to perform a review of email evidence for

relevance is unduly burdensome. *In re the Matter of the Search of Google Email Accounts*, No. 14-mj-00352, --- F. Supp. 3d ----, 2015 WL 1650879 (D. Alaska Apr. 13, 2015).

The Court issued a search warrant that "directed Google to provide the government with email correspondence from six Gmail accounts that were exchanged during brief periods of time these accounts were used to respond to Craigslist advertisements posted by [Redacted poster] @yahoo.com that solicited sexual encounters with minors." *Id.* at *1. Google resisted the warrant because it "required Google to inspect email content for relevancy and evidentiary value," that is, emails relating to the solicitation of sex with minors, and Google contended "that it is not competent to perform such an analysis, and requiring it to do so is unfair and unduly burdensome." *Id.* at *2. The Court "readily" agreed, and "absolve[d] Google from any responsibility to review email content when responding to the warrant," and specifically for "relevance and for evidentiary value." *Id.* at *2-5..

Back to Top

Vendor Developments

We are seeing some very positive--and also some rather negative--developments in the e-discovery services (aka vendor) market. The best vendors are providing an array of powerful technologies--such as predictive coding, visual analytics and machine translation--along with consistently high-quality professional services to ensure that these tools are used effectively and defensibly.

Some vendors are also beginning to provide more straightforward and simplified pricing, in lieu of the complex *à la carte* pricing of the past. Until recently, vendors typically charged separately for the use of technologies such as predictive coding, analytics and even e-mail threading--often at expensive rates--making use of these technologies impractical. We are now seeing some vendors, particularly those that have developed their own applications and therefore do not have to pass on licensing fees from separate software vendors (allowing them pricing flexibility), more frequently bundling these technologies in a single technology fee. When this bundling is priced reasonably, which we are also seeing, the use of predictive coding, analytics and other technologies that make search and review more efficient can more often be a viable option than in the past.

Some vendors are investing considerable resources to educate their existing and potential clients about the e-discovery process through white papers, webinars, seminars and blogs. Of course, some materials and programs are more sales pitch than real education. But the better materials can add significant value.

On the negative side, the market for e-discovery services remains immature. We continue to see a dizzying array of e-discovery service providers vying for market share, with ever lower barriers to entry, and a market that often appears ill-equipped either to distinguish among them or to evaluate the quality of their services, technology or pricing. Vendors that provide both cutting-edge technology and outstanding professional services appear to be a relatively rare find, as those that excel in one area too often fall short in the other. Consistency also remains an issue. Finding a vendor that consistently provides excellent service across matters and over time can seem like prospecting for gold: a lot of work and often disappointing results.

In the fog of this environment, some vendors with inferior technology and limited professional services are nevertheless able to demand premium pricing. Sales tactics have grown increasingly aggressive, with direct sales calls to individual (often inexperienced) lawyers at firms and companies, and enticements being offered in exchange for attending demos.

One of the more troubling new developments has been some vendors' attempts to, in effect, "consumerize" e-discovery--*i.e.*, to sell e-discovery software as a service (SaaS) directly to end users (*e.g.*, individual lawyers) much like an app, with little or no professional services component involved. The origins of this consumerization movement may be traceable to some major vendors' cloud-based e-discovery offerings. Vendors offering these cloud-based e-solutions typically target law firms and companies with professional litigation support staff with the skills to manage complex projects and execute difficult tasks. The consumerization approach, by contrast, directly targets individual lawyers and rests on a sales pitch that implies e-discovery is easy. The problem is that all too often, even with the best technology, it isn't, and the risks and consequences of failure, as always, remain great (see our sanctions discussion above).

Back to Top

Federal Rule Amendments

For those old enough to remember, there's a scene in the film *Monty Python and the Holy Grail* in which Sir Lancelot is seen charging across a field to attack a castle. The camera pans back and forth between two guards posted at the front of the castle and Lancelot, who each time is still where he started, endlessly charging forward but getting nowhere. The drawn-out process to implement a second round of e-discovery related amendments to the Federal Rules of Civil Procedure (the first round was in 2006) has, at times, felt a lot like that scene.

It started with the Civil Rules Advisory Committee's Duke Litigation Review Conference in 2010, followed by a series of public meetings and a "Mini-Conference" in 2011, after which the Committee in August 2013 released a set of proposed rule amendments for public comment. After the public comment period, which included 120 testifying witnesses and over 2,300 written comments, the Discovery Subcommittee of the Civil Rules Advisory Committee submitted a revised proposal, which the Civil Rules Advisory Committee adopted in April 2014. The Judicial Conference approved the proposed amendments on September 16, 2014, and forwarded them to the Supreme Court, which adopted them on April 29, 2015, and sent them to Congress. Absent Congressional action, the proposed amendments will become effective on December 1, 2015.

The proposed amendments affect Federal Rules of Civil Procedure 1, 4, 16, 26, 30, 31, 33, 34, 37, 55 and 84. The most significant for e-discovery purposes are the proposed amendments to Rules 37(e) (sanctions), 1 (cooperation) and 26(b)(1) (proportionality and scope of discovery).

Sanctions for Failure to Preserve ESI (Rule 37(e))

The most anticipated of the proposed amendments is that to Rule 37(e), which will govern the imposition of sanctions for failures to preserve electronically stored information that a party had a duty

to preserve. The amendment is primarily intended to address inconsistencies in the level of culpability courts have applied in imposing the most serious sanctions, such as case termination or an adverse inference instruction, and the perceived unfairness of sanctioning a party that has acted reasonably yet some ESI has nevertheless been lost. It also seeks to address the problem of over-preservation--*i.e.*, parties preserving too much information because of fears of harsh or case-terminating sanctions.

The proposed amendment provides: "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."

The Advisory Committee Note states that by specifying the measures that a court may employ if ESI is lost and the findings it must make, the proposed amendment to Rule 37(e) "forecloses reliance on inherent authority or state law to determine when certain measures should be used." *See* Advisory Committee Note at 38.

The proposed amendment creates a safe harbor if a party acted reasonably to preserve ESI. *See* Thomas Y. Allman, *Thoughts on the 2015 Amendments to Federal Rule of Civil Procedure 37(e),* 15 Digital Discovery & e-Evidence 245 (June 11, 2015). If a party demonstrates that it took "reasonable steps" to preserve, no sanctions or other remedies are available under the proposed rule, even if ESI was lost. The Committee Note expressly states that "[b]ecause 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." *See* Advisory Committee Note at 41.

Significantly, the Committee Note also expressly encourages to courts to consider proportionality in determining whether a party's preservation efforts were reasonable. Recognizing that "aggressive preservation efforts can be extremely costly," the Note states that "[a] party may act reasonably by choosing a less costly form of information preservation, if it is substantially as effective as more costly forms." *Id.* at 42.

Only if a party has failed to take reasonable steps to preserve ESI that should have been preserved, and the information is lost as a result, then the proposed amendment provides that the focus should be on whether the lost information can be restored or replaced through additional discovery. If the information is restored or replaced, no further measures should be taken. The Committee Note states that "[a]t 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." *See id.*

If the lost ESI cannot be restored or replaced through additional discovery, the court must find that the other party has been prejudiced before imposing any curative measures or sanctions. According to the Committee Note, "[a]n evaluation of prejudice from the loss of information necessarily includes an evaluation of the information's importance in the litigation." *Id.* at 43. Once a finding of prejudice is made, only then is the court authorized to employ measures "no greater than necessary to cure the prejudice." *Id.* The court may impose specified very severe measures--*i.e.*, an adverse inference or a case terminating sanction--only if the court finds that the party acted with the intent to deprive the other party of the information's use in the litigation.

Given the December 1, 2015 effective date for the proposed rule amendments, we likely will not know until at least mid-2016 (or later) whether the amendment to Rule 37(e) appears to be fulfilling its goals in practice and can bring more fairness to the e-discovery sanctions area. One important area that it does not address is the trigger for the duty to preserve, for which there is a split in the courts. In the Seventh Circuit, such a duty is triggered only when litigation is "imminent." Everywhere else, it is triggered where courts find that litigation was "reasonably foreseeable."

Cooperation (Rule 1)

The proposed amendment to Rule 1 was originally crafted to require cooperation among the parties, but that language was dropped relatively early on out of concerns that it would only spawn tangential disputes regarding whether parties were being sufficiently cooperative.

In its final proposed form, amended Rule 1 provides that the rules of civil procedure would not only be "construed and administered" (the current language) but also "employed by the court and the parties" to secure the just, speedy, and inexpensive determination of every action and proceeding.

The concept of cooperation still made it into the Committee Note that accompanies the proposed amendment, which states that "effective advocacy is consistent with – and indeed depends upon – cooperative and proportional use of procedure." *See* Committee Note at 1-2.

Proportionality and the Scope of Discovery (Rule 26(b)(1))

The amendment to Rule 26(b)(2)(C)(iii) moves the proportionality factors from Rule 26(b)(2)(C)(iii) to Rule 26(b)(1).

As amended, Rule 26(b)(1) would permit a party to obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense "and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit."

The intended effect of this reorganization is to strengthen the concept of proportionality in courts' consideration of the permissible scope of discovery. The Committee Note states that the movement of the proportionality factors from Rule 26(b)(2)(C)(iii) to Rule 26(b)(1) "restores" them "to their original

place in defining the scope of discovery" and "reinforces" the "obligation of the parties to consider" them "in making discovery requests, responses or objections." *See* Committee Note at 19.

Back to Top

International E-Discovery Developments

The cross-border transfer and disclosure of information remains a hot topic in e-discovery in Europe and the Asia Pacific region.

Adequacy of US-EU Safe Harbor Program Challenged

On March 24, the European Court of Justice (ECJ) heard arguments in a case challenging the US-EU Safe Harbor Framework, which allows certified US companies to send personal data outside Europe if they meet certain European Union requirements.

In *Maximillian Schrems v. Data Prot. Comm'r*, activist Max Schrems argued that the Irish Data Protection Agency (DPA) did not properly investigate his claims that Facebook violated European data privacy rules by transferring European users' data to US-based servers, making the data accessible to the National Security Agency for its PRISM program. The Irish DPA rejected Schrems' claim without further investigation because of Facebook's Safe Harbor certification. Schrems sued the DPA in the Irish High Court, which referred his case to the ECJ.

The ECJ must decide whether the Irish DPA was correct in relying on Facebook's Safe Harbor status, or whether the Safe Harbor Framework does not at present ensure adequate data privacy protection for European citizens' data. At the March argument, the European Commission defended the Framework. The Commission conceded that at present there is no guarantee that EU citizens' data will be adequately protected, but emphasized that the Safe Harbor Framework is important for maintaining political and economic ties to the United States and US-based companies.

In the meantime, the Safe Harbor Framework is in the process of being amended to increase transparency and more actively enforce compliance, though the US and EU negotiators have yet to reach an agreement on the terms of the amendments.

Cross-Border Transfer and Disclosure of Information Remains a Hot Topic in the Asia Pacific Region

Cross-border transfer and disclosure of information remains a hot topic in the Asia-Pacific region. "Data localization laws"--laws mandating that certain industries store data within a country's borders--such as China's State Secret laws are of particular concern to companies.

In the case of China, the law prohibits the export of electronic data concerning "state secrets," a term that is defined broadly by statute and by Chinese enforcement authorities implementing the laws. Notably, a 2014 Hong Kong decision interpreting the law ruled that it does not amount to a blanket prohibition against cross-border data transfers. Despite this, the broad scope of the law and harsh

penalties levied for violations have increasingly led companies to keep their data in China, and to rely on mainland Chinese law firms to assist with handling of data and document review.

Back to Top

Conclusion

We're off to a fast start in e-discovery this year. Look out for our articles, client alerts and our year-end update in January 2016.

Gibson Dunn & Crutcher's lawyers are available to assist in addressing any questions you may have regarding the issues discussed in this update. The Electronic Discovery and Information Law Practice Group brings together lawyers with extensive knowledge of electronic discovery and information law. The group is comprised of seasoned litigators with a breadth of experience who have assisted clients in various industries and in jurisdictions around the world. The group's lawyers work closely with the firm's technical specialists to provide cutting-edge legal advice and guidance in this complex and evolving area of law. For further information, please contact the Gibson Dunn lawyer with whom you usually work or the following leaders of the Electronic Discovery and Information Law Practice Group:

Gareth T. Evans - Orange County (949-451-4330, gevans@gibsondunn.com)
Jennifer H. Rearden - New York (212-351-4057, jrearden@gibsondunn.com)
G. Charles ("Chip") Nierlich - San Francisco (415-393-8239, gnierlich@gibsondunn.com)