ISSUE
01
April
2013

Quarterly report of case law and trends in eDiscovery

BABC eDiscovery Newsletter

this issue

BABC's eDiscovery Team

BABC's eDiscovery team is comprised of attorneys from various practice groups, and has significant experience with eDiscovery issues across a broad spectrum of cases. The team provides this quarterly report to highlight important cases and issues that impact litigation practice in the digital world.

Team Attorneys

Ty Dedmon - Chair
Jonathan Head - Co-Chair
David Deusner - Editor
Brie Buchanan
Kyle Hankey
Jessica Jones
Riley Key
Ann Phelps
Avery Simmons
Max Smith
Fritz Spainhour
Frankie Spero

Case Insights

Peerless Industries, Inc. v. Crimson Av, LLC, Case No. 1:11-cv-1768, 2013 U.S. Dist. LEXIS 2985 (N.D. Ill. Jan. 8, 2013)

eDiscovery Issue: Reliance on Vendor to Oversee Collection from an Affiliated Company Was Insufficient

The district court sanctioned the defendants, Crimson AV, LLC and its managing director, for failing to produce relevant documents and electronically stored information (ESI) within the possession and control of an affiliated company, Sycamore Manufacturing Co., Ltd., which was not a party to the lawsuit. The plaintiff, Peerless Industries, Inc., asserted that most of the documents and ESI relevant to Peerless' claims against the defendants were located on Sycamore's servers and in Sycamore's files. Accordingly, pursuant to Rule 34 of the Federal Rules of Civil Procedure, Peerless filed a request to deem documents in the possession and control of Sycamore within the possession and control of the defendants. The district court, in granting Peerless' request, concluded that because the president of Sycamore was a principal of both Crimson and Sycamore and exercised a considerable amount of financial and managerial control over both companies, Crimson was deemed to be in control of the relevant Sycamore documents and information and therefore was able to obtain the relevant documents from Sycamore.

After the defendants failed to produce the requested Sycamore documents, Peerless filed a motion to compel, at which point the defendants agreed to produce all responsive documents in lieu of an order by the court. But rather than producing responsive documents, the defendants responded by stating that any documents responsive to Peerless' requests had either already been produced in the litigation, no longer existed, or could not be found. However, at the subsequent Rule 30(b)(6) deposition of Crimson's representative, Peerless learned that the defendants had not conducted a reasonable investigation regarding their production of the relevant Sycamore documents. Crimson's representative was "unable to answer questions about Sycamore's computer and backup systems, what searches were performed, which employees would have relevant information, whether a document hold had been implemented, or whether employees at Sycamore were even contacted regarding [Peerless'] document requests." Following the Rule 30(b)(6) deposition, Peerless filed a motion for economic sanctions based on the defendants' failure to produce the relevant Sycamore documents.

The district court pointed to its prior order holding that the defendants were "'able to obtain the relevant documents Sycamore' requested because [Sycamore's president] was [a] principal of both Crimson and Sycamore and that he exercised a considerable amount of control over both corporations." According to the district court, that prior order "of course required defendants to contact individuals at Sycamore and play a role in obtaining the necessary discovery." The district court found, however, that the defendants did not "play a role," but instead "took a back seat approach" and allowed the document investigation to proceed entirely through a "vendor." In other words, the defendants "had no part in the process of obtaining the requested discovery or of determining how Sycamore managed their documents and what might be relevant to [Peerless'] requests." The district court held that such a "hands-off approach" to an investigation for responsive documents is insufficient. The defendants could not satisfy their burden to produce the requested documents by "placing the burden of compliance on an outside vendor and have no knowledge, or claim or control, over the process."

Accordingly, because the defendants had failed to properly investigate and respond to Peerless' requests for the relevant Sycamore documents, the district court granted Peerless' motion for economic sanctions. The district court held that the "[d]efendants must show that they in fact searched for the requested documents and, if those documents no longer exist or cannot be located, [then] they must specifically verify what it is they cannot produce."

The Peerless case highlights two important points. First, under Rule 34 of the Federal Rules of Civil Procedure, a responding party must produce any responsive documents, ESI, and tangible things in its "possession, custody, or control," which could include documents, ESI, and tangible things in the possession, custody, or control of an affiliated non-party (e.g., sister company, subsidiary) depending on the degree of the connection between the responding party and the affiliated non-party. Second, in conducting its search and investigation for responsive documents, ESI, and tangible things—particularly ESI—a responding party may not merely rely upon an outside vendor to conduct the investigation. Rather, the responding party must take a "hands-on" approach and play an active role in searching for responsive documents and ESI and determining which documents and ESI no longer exist or cannot be located and ,therefore, cannot be produced. Failure by the responding party to take such an active role in its search for responsive documents and ESI may result in a ruling against the responding party that it did not meet its burden under Rule 34 and an award of economic sanctions against the responding party.

Gabriel Technologies Corp. v. Qualcomm Inc., Civ. No. 08cv1992 AJB (MDD), 2013 U.S. Dist. LEXIS 14105 (S.D. Cal. Feb. 1, 2013)

eDiscovery Issue: $2.8 Million in Fees Awarded to Prevailing Party for its Computer Assisted Review Costs

U.S. District Judge (S.D. Cal.) Anthony J. Battaglia recently awarded over $2.8 million in attorneys' fees and costs for using predictive coding and over $391,000 for document review services.

Plaintiffs filed suit in 2008 for 92 patent violations and 11 causes of action. After four amended complaints and extensive discovery, plaintiffs narrowed their claims to 16 patents. During the case, the court approved an $800,000 bond, which the plaintiffs posted in order to avoid dismissal of their claims. Later, the court granted summary judgment as to all of plaintiffs' claims. The defendants filed a motion for attorneys' fees and costs under federal law (fees and costs to the prevailing party in "exceptional" patent cases) and state

EDISCOVERY CONCEPTS TO KNOW

PST (Outlook Personal Storage Table): A PST file is most commonly associated with Microsoft's email software, Outlook. It is typically associated with smaller organizations that do not utilize Microsoft's email server, Exchange. Users may also use PST files to store messages on local workstations or network file shares, usually as a space-saving technique. PST files are also commonly used to store and transmit select, individual email messages from search results to counsel.

MSG (Individual Email File): MSG is the file extension for Outlook's email application. An MSG file can contain the message and attachments. MSG messages can be saved like any other file type simply by dragging to another folder or location, on a network file share or external device. MSG files are typically the most common format for emails in ediscovery.

EML (Individual Email File): An EML email file is commonly associated with Outlook Express and similar to an MSG file.

FAMILY RELATIONSHIP: This term generally refers to two or more documents that are related. The most common example of a family relationship is an email and corresponding attachment. In the ediscovery context, it may also refer to embedded files which are extracted from other files as part of the processing phase. Related terms include "Parent" and "Child" to refer to the relationship between the documents comprising a family. In the example of an email and a related attachment, the email is generally referred to as the Parent and the attachment is referred to as the Child.

law (fees and costs for filing a misappropriation claim in bad faith). Judge Battaglia decided that the plaintiffs made frivolous claims in bad faith, making the case "exceptional," and awarded fees and costs under both statutes. The court considered evidence including its own warning that the case lacked merit during the bond hearing and emails suggesting the plaintiffs knew they lacked requisite evidence.

Specifically, the court approved attorneys' fees of $10,244,053, including $2,829,349.10 for using a document review algorithm developed by H5, an eDiscovery firm. The algorithm sorted 12,000,000 records into responsive and non-responsive documents, which an outside vendor then reviewed.

The court found H5's computer-assisted review to be a "more efficient and less time consuming method of document review" that "seemingly reduced the overall fees and attorney hours." Finally, the court sanctioned the plaintiff's law firm for its total billing, $64,316, to erase any profit and deter frivolous filings. Note that the plaintiffs did not object to the reasonableness or amount of the sanctions.

"The Court finds the Statement of Work (SOWs) ...by Defendant to be persuasive, credible, and reliable considering the work to be done to search and extract any relevant emails."

EEOC v. The Original Honey Baked Ham Company of Georgia Inc., 2013 U.S. Dist. LEXIS 26887 (D. Colo. Feb. 27, 2013)

eDiscovery Issue: Court Grants Access to Class Members' Social Media Accounts

Where social media, text messages, blogs, and emails are relevant, at least one court has ordered production of social media usernames and passwords for all class members and examination of accounts by a forensic expert. This court required a class of plaintiffs asserting discrimination to produce three years of text messages, email messages, and access to their online media accounts.

The EEOC filed Title VII suits against The Original Honey Baked Ham Company of Georgia on behalf of a class of female employees. In discovery, Honey Baked Ham moved to compel production of the plaintiffs' Facebook accounts and text messages. Honey Baked Ham proved that the information was relevant using the named plaintiff's Facebook account.

The court examined the postings on the named plaintiff's Facebook account and found "musings about her emotional state in having lost a beloved pet as well as having suffered a broken relationship; other writings addressing her positive outlook on how her life was post-termination; her self-described sexual aggressiveness; [and] statements about actions she engaged in as a supervisor with Defendant" were relevant.

The court ordered every plaintiff to produce Facebook account information, cell phone records, and emails for three years. To preserve privacy and address confidentiality concerns, the court created a questionnaire to gather only relevant account information. Plaintiffs were to provide hard copy responses for review before production to Honey Baked Ham.

"[P]laintiff's counsel had done little, or nothing, in terms of a reasonable inquiry and indeed had no knowledge of the number and identity of responsive documents ... the Court concludes that Branhaven failed to make a reasonable effort to assure that the client has provided all the information and documents responsive to the discovery demand ... misled the opposing party and the Court in its certification, and did not comply with Fed. R. Civ. P. 34."

Optiver Australia Pty. Ltd. v. Tibra Trading Pty. Ltd., Case No. C 12-80242 EJD (PSG), 2013 U.S. Dist. LEXIS 9287 (N.D. Cal. Jan. 23, 2013)

eDiscovery Issue: SCA Prohibits Searching Google Email

Newspapers these days are full of articles, both factual and conspiracy-laden, about how various email service providers (Google always manages a prominent mention) freely and frequently disclose our private electronic data to federal investigators. Perhaps this is appropriate in some cases, but parties should know that a very different standard, affirmed in a recent California case, applies to private litigants. That court wrote, in its opinion denying most of the discovery sought, "The Stored Communications Act (SCA) offers broad protection against disclosure of content by service providers." After obtaining discovery, Optiver contended that Tibra's disclosures were incomplete and sought discovery in U.S. courts. Optiver specifically wanted to see whether Tibra sent emails using PGP encryption, which wasn't used within the company and would suggest foul play.

Optiver subpoenaed Google, the email custodian, for three different items. First, it wanted emails from Tibra employees that contained the terms "PGP" or "Optiver." The court denied this request based on the text of the SCA, which prevents it from disclosing electronic "content," defined as "any information concerning the substance, purport, or meaning of that communication." Second, Optiver sought and was denied access to the subject lines of emails for the same reason. Last, Optiver sought and recieved "non-content metadata" that might reflect when Tibra created the accounts and used them rather than reflecting the emails' substance. Given the denial of the first two requests, the court was dismissive in allowing the relief. However, it is worth asking why the date of an account's creation and certain other metadata—take for instance, the timing of when Tibra sent most emails; late at night could suggest foul play — are not protected similarly.

This case follows many others that prevent litigants from doing an end-around by subpoenaing a service provider, though any good litigator will tell you the truth often only emerges through multi-sourced discovery. Accordingly, litigants are well positioned when they focus your efforts on thorough discovery protocols and disclosures in the earliest possible stages of litigation.

Christou v. Beatport, LLC, Civil Action No. 10-cv-02912-RBJ-KMT, 2013 U.S. Dist. LEXIS 9034 (D. Colo. Jan. 23, 2013)

eDiscovery Issue: Failure to Preserve Text Messages

The United States District Court for the District of Colorado recently sanctioned a defendant for failing to preserve text messages. The plaintiff, Regas Christou, founded several nightclubs in Denver specializing in electronic dance music. One of the defendants, Bradley Roulier, previously booked acts for the nightclubs. After Roulier started a competing nightclub, Christou filed suit against Roulier contending that Roulier was using his influence as the founder of his website to discourage top acts from performing in Christou's nightclubs.

After filing suit, the paintiffs asked the defendants to preserve potentially relevant documents, including text messages. However, defendants did not preserve text messages on Roulier's iPhone and did

not produce any text messages in response to the plaintiff's first discovery requests. Roulier later lost his iPhone with all the text messages on it. As a result, the plaintiffs requested that the courts sanction the defendants.

The defendants responded that because Roulier testified he did not use text messages to book acts, it was speculation that text messages were relevant. However, the court noted that the mere fact that Roulier did not book acts via text message was hardly proof that the text messages were irrelevant. While defendants stated they "found no responsive text messages," they failed to indicate whether defense counsel actually reviewed Roulier's iPhone at all. More importantly, because the defendants had a duty to preserve text messages, few as they might have been, but failed to do so, no one would ever know whether they were relevant. Because the defendants had a duty to preserve the text messages, the court found that sanctions were proper.

Preservation of ESI can be challenging. Companies increasingly rely on technology to conduct business and communicate. Regardless of the size of the case or amount at issue, counsel must consider a wide variety of potentially relevant storage devices.

In the absence of an agreement to the contrary counsel should account for and preserve all potentially responsive data sources, including smartphones.

"I view this content logically as though each class member had a file folder titled 'Everything About Me,' which they have voluntarily shared with others."

Equal Employment Opportunity Commission v. JP Morgan Chase Bank, N.A., No. 2:09-cv-864, 2013 U.S. Dist. LEXIS 27499 (S.D. Ohio Feb. 28, 2013)

eDiscovery Issue: Failure to Preserve Database Data

In this case, the court imposed sanctions for the destroying database data. Skill login codes, according to the order, indicate what skills the defendant assigned to individual mortgage consultants. These assignments control into what call queue a mortgage consultant is placed. These records also would indicate the time at which a consultant logs into the system to receive incoming calls. The plaintiff said statistical analysis of this data could show discrimination based on how these calls were allocated among consultants.

The defendant conceded that it destroyed data during routine purging of electronic data. (In a bad sign, defendant had first argued that Plaintiff failed to comply with Rule 37's certification requirement, which only applies to a motion for sanctions for failing to answer or respond.) The court disagreed, holding, "The defendant's conduct constitutes at least negligence and reaches

Case Updates

for willful blindness bordering on intentionality." As sanctions, the court denied the defendant's motion for summary judgment and ordered an adverse inference be instructed to the jury. A magistrate judge ordered the production of the data.

Connecticut General Life Insurance Company v. Earl Scheib, No. 11-CV-0788-GPC (WVG), 2013 U.S. Dist. LEXIS 16234 (S.D. Cal. Feb. 6, 2013)

eDiscovery Issue: Email Production Deemed Too Costly Applying Cost-Benefit Analysis

Litigators (and clients alike) often complain about the cost of producing emails. To be sure, it is often costly even in small matters. In this case, the defendant came armed with "persuasive, credible, and reliable" numbers to support its claim that the cost of producing 219 GB of email outweighed the benefits to the plaintiff, and the court agreed.

The defendant objected to a new production request because producing was unduly burdensome. The defendant represented during a discovery conference that production would cost approximately $120,000 (the same amount at stake in the matter). The court ordered the defendant to prove the cost breakdown associated with searching for and producing responsive documents, along with cost estimates for alternative searches, such as the cost breakdown associated with producing only relevant emails from witnesses to be deposed.

In its supplemental briefing, the defendant did just that. It provided the court with a vendor estimate that showed that the searching alone would cost well over $120,000. The court considered the Statements of Work – standard eDiscovery industry documents – with details of the vendor's proposed work and cost estimates to be persuasive, credible, and reliable. Even reducing the scope to just individuals plaintiff had noticed for depositions would cost over $30,000.

Although the information sought by the plaintiff's may have been helpful, applying the cost-benefit analysis proved that spending this type of money to produce emails in response to five requests, given the defendant's ongoing production related to other request , was not justified. Be prepared to show the court real numbers to back up your claims of undue burden and you'll stand a greater chance of winning your challenge.

"DELETED" EMAILS: Just because a user deletes an email from her inbox does not mean it no longer exists. In most Outlook configurations, the act of deletion moves the email from one's Inbox (in Outlook) to the Deleted Items folder. If the email system creates a backup and the user has not emptied the Deleted Items folder, the backup will generally contain a copy of the "deleted" email that may be subject to discovery. A copy may also reside on the central server for additional time before being ultimately wiped forever.

DUPLICATE EMAILS: When a user sends an email to multiple people, an exact copy of that email exists in each recipient's inbox. If there are many recipients and if the recipients reply to all other people on the email chain, then many, many duplicative emails are created. Deduplication prior to attorney review does not harm the dataset and can vastly reduce the impact of numerous duplicates on the cost and consistency of the review. Deduplication is topic that attorneys should address and agree upon prior to commencing review.

eDiscovery 101

Q: What are some concrete steps to reduce the cost associated with ediscovery?

A: With 98% of all corporate data now created electronically, virtually all cases will include some form of electronic data to be produced. By limiting the scope of the data that will be preserved and searched for responsiveness, you can significantly reduce the exposure and costs associated with producing ESI.

Our team has significant experience advising our attorneys on reaching agreement on the scope of ESI, generally through an "ESI Protocol" incorporated into the Case Management Order or similar order.

Limiting the number of custodians, the date range, file types and sources of data , as well as specifying certain repositories as "not reasonably accessible" are all ways you can reduce the burden associated with electronic discovery.

ESI Protocols can vary greatly by client and by case, so ask a member of our ediscovery team how one can be prepared for your next matter.

HOW MUCH DATA IS THAT?*

1 GB is about 75,000 pages (pick-up truck full of documents).

Average pages per email: 1.5 (100,099 pages per gig)

Average 1GB PST file is 9,000 emails and 3,000 attachments.

**Numbers vary for any given dataset, and there is disagreement as to these figures in the ediscovery industry; generally speaking, the preceeding serve as a good baseline for understanding the size and composition of your data.*

babc.com

EXTRACTED TEXT: Extracted Text refers to the text that is derived from an electronic file, usually during the processing phase, which is utilized for performing searches within a review database.

OCR: OCR or "Optical Character Recognition," refers to the process of identifying text within a document in order to search the contents. OCR text is generally used to retrieve text from scanned images of paper documents or in instances when no text is rendered from an electronic file.

MD5 HASH: Often referred to as the digital equivalent of a fingerprint, the MD5 hash value for an electronic file is a unique value derived by applying an algorithm to the binary content of a file. In the ediscovery context, MD5 hash values are often used to identify duplicate versions of the same file, but serve significant evidentiary functions as well. Accurately identifying exact copies of files can significantly reduce the attorney review costs.

eDiscovery News
Issue 01 April 2013

Branhaven, LLC v. Beeftek, Inc., Civ. No. WDQ-11-2334, 2013 U.S. Dist. LEXIS 13364 (D. Md. Jan. 4, 2013)

eDiscovery Issue: Counsel Sanctioned for Wrongful Certification under Rule 26(G)

The court sanctioned Branhaven and its counsel for improper eDiscovery practices. First, Branhaven's counsel signed responses to requests for production containing the common boilerplate language that Branhaven "will make the responsive documents available for inspection and copying at a mutually convenient time." The problem? When she signed those responses, Branhaven's counsel had done nothing more than forward the requests to her client. She did not find out whether any responsive documents existed, much less locate them and prepare to produce them as the response suggested. Accordingly, the court found Branhaven's counsel had not made the "reasonable inquiry" required by the Federal Rules of Civil Procedure and in fact had provided a "meaningless and arguably misleading response" in an effort "to buy time and technically comply with Rule 34."

Second, after providing only 388 pages of documents in five months, Branhaven dumped over 100,000 pages of documents on the defendants just a few days before Branhaven's 30(b)(6) deposition. Moreover, Branhaven produced these documents in PDF rather than TIFF format and did not Bates-number all of the pages. Although the court found that the production was (barely) timely under the scheduling order, the volume, the timing of production, the format, and the lack of complete Bates-numbering rendered the production not "in a reasonably usable form," as required by Rule 34.

The defendants had sought to have Branhaven's documents excluded, but the court was unwilling to go that far. Instead, the court assessed Branhaven and its counsel—jointly and severally—costs the defendants incurred to convert the production to a useable format as well as the defendants' attorneys' fees associated with bringing the motion for sanctions.

A couple of lessons stand out from Branhaven's sanctions. Do not delay a diligent search for responsive documents, and certainly do not represent that you've done such a search if you haven't. Two, work cordially with your opponents to come to agree on production details. If Branhaven had produced the documents in an agreeable format—even at the last minute—it likely would have escaped sanctions.

Brookfield Asset Management, Inc., v. AIG Financial Products Corp., No. 09 Civ. 8285 (PGG) (FM), 2013 U.S. Dist. LEXIS 29543 (S.D.N.Y. Jan. 7, 2013)

eDiscovery Issue: 502(d) Stipulation Provides Absolute Right To Clawback Privileged Information

This short opinion centered on inadvertent production of privileged portions of five draft AIG Board Minutes. In a previous ruling, the court determined these minutes contained privileged information, and the defendants produced the board minutes in redacted form. However, the underlying privileged information was visible to the plaintiffs "when the corresponding metadata was reviewed."

Determining that no privilege had been waived, the court nonetheless emphasized "the need for counsel for a producing party to keep a watchful eye over their eDiscovery vendors." Secondly, the court noted that even if defendant's counsel had "dropped the ball," the parties entered into a 502(d) stipulation, which contained this salient point: "Production of any documents in this proceeding does not constitute a waiver of any applicable privilege concerning produced documents." Accordingly, despite the significance that the redacted portions might yield to the plaintiff's case or the court's admonition to scrutinize more closely its vendor's work, the stipulation provided an absolute right to AIG to claw back these documents. The court directed the plaintiff to return all copies of the draft minutes to AIG.

This case illustrates two essential points for litigators. First, a properly drafted 502(d) agreement can mitigate a significant amount of risk regarding inadvertent privilege waiver. Secondly, it highlights the importance of understanding the "form of production" of electronic documents, and the interplay between the technical aspects of producing documents and associated metadata.

Case Cites For This Issue:

Peerless Industries, Inc. v. Crimson Av, LLC, Case No. 1:11-cv-1768, 2013 U.S. Dist. LEXIS 2985 (N.D. Ill. Jan. 8, 2013)
Gabriel Technologies Corp. v. Qualcomm Inc., Civ. No. 08cv1992 AJB (MDD), 2013 U.S. Dist. LEXIS 14105 (S.D. Cal. Feb. 1, 2013)
EEOC v. The Original Honey Baked Ham Company of Georgia Inc., 2013 U.S. Dist. LEXIS 26887 (D. Colo. Feb. 27, 2013)
Optiver Australia Pty. Ltd. v. Tibra Trading Pty. Ltd., EJD (PSG), 2013 U.S. Dist. LEXIS 9287 (N.D. Cal. Jan. 23, 2013)
Christou v. Beatport, LLC, Civil Action No. 10-cv-02912-RBJ-KMT, 2013 U.S. Dist. LEXIS 9034 (D. Colo. Jan. 23, 2013)
EEOC v. JP Morgan Chase Bank, N.A., 2013 U.S. Dist. LEXIS 27499 (S.D. Ohio Feb. 28, 2013)
Conn. General Life Ins. Co. v. Earl Scheib, Inc., 2013 U.S. Dist. LEXIS 16234 (S.D. Cal. Feb. 6, 2013)
Branhaven, LLC v. Beeftek, Inc., Civ. No. WDQ-11-2334, 2013 U.S. Dist. LEXIS 13364 (D. Md. Jan. 4, 2013)

Editor's Corner

Communicating preservation obligations to employees is critical, particularly in today's corporate environment, where data is constantly in flux. Consider the following tips on implementing litigation holds to preserve data at the outset of a matter:

1. Know the Audience. A litigation hold letter should be clear and concise and drafted for its intended audience. Employees often do not understand legal concepts, so resist the temptation to draft a legal hold memorandum full of legalese. The goal of a litigation hold memo is to inform the employee of his or her obligations and to ensure data is preserved. Ensure that they understand the various forms of data they create are subject to the preservation obligation, and ask them to tell you what those are. Obtaining feedback from the employees is a good way to ensure no data is missed in your analysis.

2. Develop a Game Plan. With courts increasingly scrutinizing preservation efforts, it is essential to have a game plan in place as soon as practicable. Work with the client to ensure that one person is responsible for documenting that employees have received the notice and understand it and their duties, and address any concerns or issues they may have. Inform the IT department of the preservation obligation, and ensure that they understand the scope. Certain corporate data can be effectively preserved behind the scenes, while other data may only be known to an employee creating and storing it. Involving IT early in the process can guard against potential problems down the road, but depending on the size and makeup of the organization, employees may be holding data that IT is unaware of and does not maintain.

3. Ask Questions. Information is essential to good case planning. It is equally important to ensuring proper preservation. A best practice recommendation is to follow up with employees regarding their ESI habits through the use of an "ESI Questionnaire." These can provide invaluable feedback on issues related to use of smartphones, collaboration software, cloud services, and more. These can be disseminated along with the initial litigation hold, and are an essential tool for controlling the scope of preservation as well as informing the budget for ediscovery.