Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

eDiscovery around the globe

2015 in review

Dear Friends:

Welcome to Norton Rose Fulbright's Global e-Discovery 2015 "Year In Review" white paper.

As a global firm, representing clients in disputes across the world, we recognize that it's important that all of our litigators understand how discovery impacts our clients' cases both at home and abroad so our objective with this white paper series is to keep your organization abreast of the latest developments and trends in the fascinating world of e-Discovery.

The articles in this collection address two different aspects of discovery that we covered in 2015: Technology Assisted Review ("TAR") and Forensics. We are also including a bonus article on the amendments to the Federal Rules of Civil Procedure that went into place on December 1, 2015 in the United States.

- The first article addresses Technology Assisted Review ("TAR") and how it is being used, adopted and approved around the world.
- The second article details forensics and its place in civil discovery around the world.
- The third article summarizes the discovery amendments to the Federal Rules of Civil Procedure and how they will affect your organization.

We hope looking at these discovery issues from a global viewpoint, helps you not only solve problems in your individual cases but lets you consider these questions from the perspective of your global litigation portfolio.

Best Regards,

David J. Kessler
Chair, e-Discovery and information governance practice group

eDiscovery around the globe

A Norton Rose Fulbright whitepaper
February 2016

Global contributors

If you would like further information, please contact chair of the e-Discovery practice David Kessler.

United States

David Kessler
Partner, New York
Tel +1 212 318 3382
david.kessler@
nortonrosefulbright.com

Andrea D'Ambra
Senior Counsel, New York
Tel +1 212 318 3015
andrea.dambra@
nortonrosefulbright.com

Alex Altman
Associate, New York
Tel +1 212 318 3230
alex.altman@
nortonrosefulbright.com

Brian Evans
Assistant director of practice support, Dallas
Tel +1 214 855 8181
brian.evans@
nortonrosefulbright.com

Sam Sessler
Practice support manager, Dallas
Tel +1 214 855 8023
sam.sessler@
nortonrosefulbright.com

Australia

Abigail McGregor
Partner, Melbourne
Tel +61 3 8686 6632
abigail.mcgregor@
nortonrosefulbright.com

Michelle Isaac
Senior knowledge lawyer (disputes), Brisbane
Tel +61 7 3414 2944
michelle.isaac@
nortonrosefulbright.com

Carolyn Wyatt
National operations manager, Applied legal technology
Tel +61 8 6212 3229
carolyn.wyatt@
nortonrosefulbright.com

Canada

Lynne O'Brien
Of Counsel, Toronto
Tel +1 416 216 3923
lynne.obrien@
nortonrosefulbright.com

Europe

Marta Giner Asins
Partner, Paris
Tel +33 1 56 59 52 72
marta.ginerasins@
nortonrosefulbright.com

Enzo Lisciotto
Practice technology manager, London
Tel +44 20 7444 5382
enzo.lisciotto@
nortonrosefulbright.com

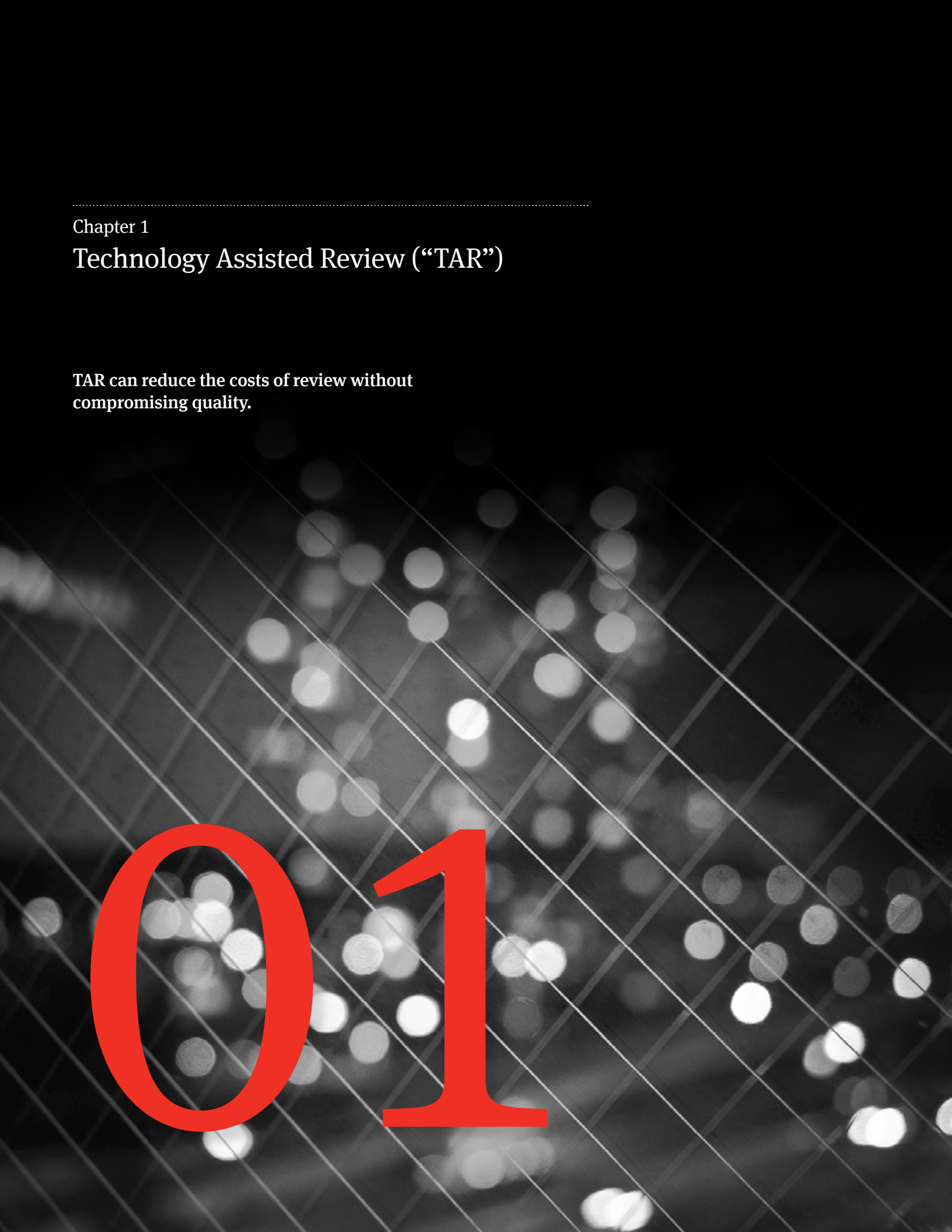
Michel Pflieger
Associate, Paris
Tel +33 1 56 59 52 74
michel.pflieger@
nortonrosefulbright.com

Contents

Chapter 1

Technology Assisted Review ("TAR")

TAR can reduce the costs of review without compromising quality.



Exponential data growth continues to swell across all industries, continually threatening the increasing costs of discovery. According to a recent IDG Enterprise 2015 Big Data & Analytics Survey,[1] small businesses currently tend to manage 1-9 terabyte (TB) of data, while many enterprises are managing 100 TB or more. Seven percent of respondents already manage more than 1 petabyte (PB) of data, and most companies are still getting most of their data from traditional sources such as databases and email. Past studies have shown that the cost of review typically consumes about 73% of all e-Discovery costs[2]. Technology Assisted Review ("TAR") can reduce the costs of review without compromising quality, by leveraging technology to apply decisions across documents instead of using only contract reviewers. To be used most effectively, TAR needs to be coupled with robust processes, documented workflow, and proper guidance and supervision by lawyers and technical resources.

What is "TAR"?

TAR is the most innovative and advanced technology to improve the transparency of document sets to speed review, reduce costs, and improve consistency and quality. Over the years, many different technologies have been developed to programmatically compare documents and either reduce the volume of documents that need to be reviewed (such as hashing and deduplication that removes exact duplicates) or group documents together because they have similar themes or concepts so they can be reviewed together (e.g. near deduplication, concept clusters, and email threading).

TAR is the next generation of this technology because it groups documents based on reviewers coding. Generally speaking, TAR analyzes the documents that reviewers have coded, looks for commonalities between those documents and then maps that coding to documents that have not been coded. At its most basic, TAR or predictive coding suggests unreviewed documents for review that it believes are important based on the coding of the reviewers.

What isn't TAR (automatic coding)?

While in theory, a party or a lawyer could simply accept TAR's suggestions without further review, it is generally not recommended that TAR's coding be automatically applied.

TAR is more accurately a computer-categorized review workflow that prioritizes documents for review, rather than to refer that a computer replaces human coding decisions. Suggested relevant documents or related analytics in nearly every situation still involve a human reviewer to perform legal analysis to confirm the documents' status. The use of "automated coding" in which computer suggested documents are accepted without human review is one that requires a thoughtful, defensible strategy and evaluation of risks and is yet to be tested by the courts.

How to use it

While there are different types of analytics and predictive coding software, the processes are similar, and yet, predictive coding software can still be trained for the purposes of a document review in several ways. One approach would involve matter expert attorneys reviewing a smaller set of documents set as "seeds" or exemplars (a.k.a. a "seed set"), that they have judged to be clearly fitting, or not fitting, the desired characteristics of various document categories. The continual building of this seed set would start from a representative random sample, which would be used to train the computer to suggest similar documents for human review. The continual learning process would be ongoing and iterative, and review of prioritized documents would continue until there are no more, or reasonably small amounts of uniquely relevant or important documents suggested. The team then determines the appropriate level of validation steps to evaluate if the remaining documents are reasonably relevant or important, and how the remainder of the documents should be handled.

1 IDG Enterprise 2015 Big Data & Analytics Survey (available at http://core0.staticworld.net/assets/2015/03/16/2015-data-and-analytics-survey.pdf).

2 Nicholas M. Pace and Laura Zakaras, Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery, http://www.rand.org/pubs/monographs/MG1208.html

Disregarding automatic coding and simply accepting the TAR suggestions, TAR can be used in two ways to identify relevant documents. First, it can be used to prioritize and set the order documents are reviewed. This still means all the documents in the review set are going to be reviewed, but the responsive documents should be toward the front. Second, TAR can be used to cull irrelevant documents. As it prioritizes and responsive documents are moved to the front, it leaves irrelevant documents behind. At a certain point, the TAR system cannot find any more relevant documents to prioritize and it may be reasonable to stop review because the benefit of review has decreased and the cost could still be significant. We generally recommend sampling this "left behind" population of documents to determine that nothing material or significant was missed by the TAR algorithm.

What are the benefits of TAR?

TAR, when deployed properly, speeds review by clustering documents together, improves quality by presenting like documents together, and reduces the documents that need to be reviewed by prioritizing the responsive documents and leaving the irrelevant documents to the end. Depending on the preferences of the clients, these remaining documents can be reviewed by cheaper reviewers or not reviewed at all because there is no reasonable reason to believe such documents are relevant.

While TAR can be used to help identify responsive documents from a client's own document, TAR can also be used effectively on electronic data to:

- Analyze an opponent's data and identify hot documents
- Quickly identify hot documents for early case assessment or internal investigations
- Identify gaps in email or custodian collections
- Assist and validate privilege identification
- Develop and test key terms

Where does TAR not work optimally?

TAR does have limitations and some examples where TAR and predictive coding may be less effective are:

- Non-searchable and low searchable text content (photos, audio/video, images, AutoCAD or design drawings)
- High numeric, low text content (spreadsheets, databases, source code and system files)
- Across multiple languages (these documents need to be analyzed in single language groups)

The United States perspective

Is TAR accepted?

Yes. Every Court that has looked at TAR has said it could be part of a reasonable discovery process to cull irrelevant documents.[3] In 2012, Judge Andrew Peck issued his opinion in *Moore v. Publicis Groupe & MSL Group*, stating that "computer assisted review is an acceptable way to search for relevant ESI in appropriate cases." 287 F.R.D. 182, 183 (S.D.N.Y.) (Peck, M.J.), *aff'd*, No. II Civ. 1279, 2012 WL 1446534 (S.D.N.Y. Apr. 26, 2012). Judge Peck went on to say that it was the process employed by the party and its counsel that was more important than the exact technology used. *Id. at* 193 ("As with keywords or any other technological solution to e-Discovery, counsel must design an appropriate process, including use of available technology, with appropriate quality control testing, to review.").

Since that time, TAR has gained wide acceptance in the United States as a cost-effective and appropriate means of culling and coding documents. See, e.g., *Dynamo Holdings Ltd. P'Ship v. Comm'r of Internal Revenue*, 143 T.C. 9, 2014 WL 4636526 (T.C. Sept. 17, 2014); *In re Biomet M2A Magnum Hip Implant Prods. Liab. Litg.*, No. 3:12-MD-2391, 2013 WL 1729682 & 2013 WL 6405156 (N.D. Ind. Apr. 18 & Aug. 21, 2013); *Kleen Prods. LLC v. Packaging Corp. of Am.*, 10 C 5711, 2012 WL 4498465 (N.D. Ill. Sept. 28, 2012).

As Judge Peck observed in his recent opinion in *Rio Tinto PLC v. Vale S.A.*, "the 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." No. 14 Civ. 3042, 2015 WL 872294 at *1 (S.D.N.Y. Mar. 3, 2015). He went on to opine that "it is inappropriate to hold TAR to a higher standard than keywords or manual review. Doing

3 While the Court in *Progressive Cas. Ins. Co. v. Delaney*, No. 2:11-cv-00678-LRH-PAL, 2014 WL 3563467 (D. Nev. July 18, 2014), found that a party could not switch from search terms to TAR in midstream, this has more to do with the process the party followed and the delay it was creating. In *Bridgestone Americas, Inc. v. Int. Bus. Machs. Corp.*, No. 3:13-1196, 2014 WL 4923014 (M.D. Tenn. July 22, 2014), the Court found that a party could switch to TAR from search terms if it followed a reasonable process. No Court and no mainstream commentator has ever said that TAR could not be used to prioritize or analyze one's own documents or an opponent's documents. The only question is whether it can be reasonably used to not produce documents that are never reviewed by a person.

so discourages parties from using TAR for fear of spending more in motion practice than the savings from using TAR for review." *Id.* at *3.

How do you use TAR in a way that it is defensible to cull?

Defensibility is all about demonstrating that the process was reasonable. That it identified the documents you were looking for and did not leave behind an unreasonable amount or quality of responsive documents. Defensibility does not require perfection.

The key is test and sample the documents that TAR is indicating are not relevant. *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 257 (D.Md. 2008) ("The only prudent way to test the reliability of the keyword search is to perform some appropriate sampling of the documents determined to be privileged and those determined not to be in order to arrive at a comfort level that the categories are neither over-inclusive nor under-inclusive."). By sampling the documents that are left behind and confirming the TAR predictions, you can document that the algorithms are not systematically excluding relevant information. *American Bar Association, Predictive Coding, ABA Section Of Litigation 2012 Section Annual Conference*, p. 8 (April 18, 2012) (available at http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/14 -1_predictive_coding_written_materials.authcheckdam.pdf) Importantly, the sample does not need to indicate that no relevant documents are being left behind, but rather there is not an unreasonable amount or key documents in the sample. *See Moore*, 287 F.R.D. at 187. ("The Court reminded the parties that computer-assisted review works better than most of the alternatives, if not all of the [present] alternatives. So the idea is not to make this perfect, it's not going to be perfect. The idea is to make it significantly better than the alternatives without nearly as much cost.")

Do you have to disclose your use of TAR?

Although no court has required the parties to disclose whether they are using Technology Assisted Review, many parties have chosen to do so (when culling documents) to avoid (or at least front load) any disputes regarding this issue. Under FRCP 26(f), parties are to discuss various issues regarding the scope and conduct of discovery during their first meet and confer. Even if a party does not want to volunteer that they are using TAR, many opponents ask if they are, so it is a difficult question to avoid.

Although an opponent may often wish to inquire as to whether a party will be utilizing TAR, because the 26(f) conference comes so early in the process – before discovery is served and before the parties have a good understanding of the volume of documents implicated by the case – it is difficult for most parties to say whether they will use TAR to cull their documents. Depending on the quality and precision of search terms and the volume of data at issue, a party may decide only to use TAR to prioritize and not to cull.

Do you have to disclose your "Seed Set"?

One contentious issue that has emerged in recent years is whether a party must disclose its seed set (i.e., the documents used to train the TAR engine). In some cases, courts have required that the requesting party have access to the non-privileged responsive and non-responsive documents that comprised the producing party's seed set. See, e.g., *Federal Housing Finance Agency v. HSBC North America Holdings Inc.*, Case Nos. 11 Civ. 6189-6190, 6193, 6195, 6198, 6200-6203, 6739, & 7010 (S.D.N.Y. July 24, 2012). In most other cases, the party proposing to utilize TAR has volunteered to disclose their seed set. *See Bridgestone Ams., Inc. v. IBM Corp.*, No. 3:13-119b, 2014 WL 4923014 (M.D. Tenn. July 22, 2014); *In re Actos (Pioglitazone) Prods. Liab. Litig.*, No. 6:11-MD-2299, 2012 WL 7861249 (W.D. La. July 27, 2012) (where parties agreed that seed set coding would be done by experts from each side); *Moore*, 287 F.R.D. at 187 (where defendant volunteered to turn over all non-privileged documents from the seed set).

The tide seems to be shifting, however. Starting with a decision in In re Biomet, and most recently in Judge Peck's *Rio Tinto* opinion, the courts have found no authority permitting courts to require a party to share its seed set. ***Rio Tinto***, 2015 WL 872294, at *2; *In re Biomet M2a Magnum Hip Implant Prods. Liab. Litig.*, 2013 WL 6405156. Another well respected jurist in the e-Discovery community, retired Judge John Facciola, recently co-authored a law review article arguing that seed set documents may be privileged work product. "Safeguarding the Seed Set: Why Seed Set Documents May Be Entitled To Work Product Protection," 8 Fed. Cts. L. Rev. 1 (2015).

Can you use TAR and search terms together?

There has also been significant debate about whether parties can use search terms before utilizing TAR. The benefit of employing search terms is that it reduces the document population (and therefore the cost) of collecting, ingesting and processing data into the TAR platform. Opponents to

this practice argue that it skews the document population, potentially leaving out large numbers of documents that would otherwise have been identified as relevant by the TAR engine. This was the argument in In re Biomet, where the Plaintiff's steering committee objected to Biomet's reliance on key word searching to reduce the initial volume of documents to be reviewed before further processing using technology assisted review. The court in that case declined to require Biomet to redo its processing using the entire unculled body of data, holding that Biomet had complied with its discovery obligations. *In re Biomet*, No. 3:12-MD-2391, 2013 WL 1729682 (N.D. Ind. Apr. 18, 2013).

Another court in *Bridgestone Americas, Inc. v. Int. Bus. Machs. Corp.*, No. 3:13-1196, 2014 WL 4923014, at *1 (M.D. Tenn. July 22, 2014) reached the same decision stating although permitting the Plaintiff to "switch horses in midstream" he felt the decision warranted as the Plaintiff had agreed to openness and transparency by agreeing to disclose its seed set. Contrary to the *Bridgestone and Biomet* cases, the court in *Progressive Cas. Ins. Co. v. Delaney* case held that where the parties had initially agreed to utilize search terms to identify potentially responsive documents, a party could not later decide to use TAR to further reduce the potentially responsive population. No. 2:11-cv-00678-LRH-PAL, 2014 WL 3563467 (D. Nev. July 18, 2014).

The Canadian perspective

Is TAR accepted?

There is no definitive answer as to whether TAR is accepted in Canada. However, the Sedona Canada Principles suggest that TAR may be an effective and useful tool to assist with the review of a large number of electronic documents. Sedona Canada Principle # 7 states that:

> A party may satisfy its obligation to preserve, collect, review and produce electronically stored information in good faith by using electronic tools and processes such as data sampling, searching or by using selection criteria to collect potentially relevant electronically stored information.[4]

TAR arguably falls under the umbrella of data sampling and Canadian law firms have used TAR in document intensive, complex commercial litigations.[5] In Palmerston Grain, the court held that failure to apply the Sedona Principles to e-Discovery at large was a breach of the Ontario Civil Procedure Rules.[6] Notably, TAR has not been addressed by even one Canadian Court.

TAR & proportionality In Canada

In Canada, "the reasonable costs of preserving, collecting and reviewing electronically stored information will generally be borne by the party producing it." Sedona Canada Principle 12 places the burden of the costs of production on the producing party.[7] Further, in Todd Murphy, the Court held that "the burden, cost, and delay of the production must be balanced against the probability of yielding unique information that is valuable to the determination of the issues."[8]

Since TAR is a useful e-Discovery tool, and, since the defendant generally bears the cost of production, based on the principle of proportionality, Canadian Courts will likely look favourably on the use of TAR where its cost does not outweigh its benefit.

The European perspective

Information Management in the EU

Given the massive amounts of electronic information exchanged within the frame of administrative and judiciary procedures, solutions like the "Technology Assisted Review" (TAR) are increasingly attractive for burdened parties.

In Europe, information management issues are, in principle, less discovery-related than in the US, since most EU Member States, as well as law at the EU level, are not discovery-based. However:

- even in non-discovery countries, issues relating to the use of technologic tools such as TAR may also be key especially within the frame or in view of litigation, since parties are producing or requesting increasing volumes of data;

4 The Sedona Conference Working Group 7, The Sedona Canada Principles: Addressing Electronic Discovery, 2d ed (public comment version) (2015); see also The Sedona Conference Working Group 7, The Sedona Canada Principles: Addressing Electronic Document Production (2008)

5 See Wortzman Nickle http://www.wortzmannickle.com/wp-content/uploads/2013/11/Technology-Assisted-Review-Final-Paper.pdf.

6 Palmerston Grain, A Partnership v Royal Bank of Canada, 2014 ONSC 5134 at paras 45-46 [Palmerston Grain]).

7 Sedona Principles, supra at iv (see principle 12).

8 Murphy v Bank of Nova Scotia, 2013 NBBR 316 at paras 26, 30 [Murphy].

- law enforcement agencies, and in particular the European Commission, have extensive investigative powers, which may result in a de facto discovery, for example through massive requests for information (RFIs), in which procedural rules are less clearly defined than in a discovery-based country.

Fully aware of these pitfalls, IT experts are increasingly recommending to use appropriate tools, such as TAR, in order to facilitate and rationalize data treatment.

TAR in discovery-based countries

A very recent judgment of the High Court of Ireland appears to be the first precedent on the use of TAR in litigation (Irish Bank Resolution Corp ltd & ors v QUINN & ors [2015] IEHC 175 (3 March 2015). In this case, the High Court had previously ordered disclosure of a massive number of electronic documents in the possession of one of the parties, IBRC, but a dispute arose as to whether the disclosure should be done using TAR (method proposed by IBRC) or a traditional manual method of discovery.

In its judgment, Mr. Justice Raymond Fullam partly relied on US precedents to approve IBRC's application to be allowed to use a TAR process saying he was "satisfied that, provided the process has sufficient transparency, TAR using predictive coding discharges a party's discovery obligations under Irish law."

TAR has thus been recognized as a mean to uphold the administration of justice in a manner which is equitable and *"encompasses the objectives of expedition and economy,"* in accordance with Mr. Justice Fennelly's words in *Ryanair Plc v. Aer Rianta CPT* (2 December 2003).

This clear ruling may encourage parties, in Ireland, but also in other countries, to use TAR in litigation and may pave the way for similar decisions providing guidance on the way to use it.

For example, to date, TAR has been used infrequently in litigation in the UK. However, several recent legal changes may encourage its use:

- following to the Jackson Reforms (April 2013), the presumption in favor of standard disclosure has been replaced by a "menu" of disclosure options in multi-track cases (see Civil Procedure Rule 31.5(7)). A court is now expressly entitled to order the disclosure it considers appropriate to the case.

- according to Practice Direction 31.B on Disclosure of electronic documents, when considering disclosure of Electronic Documents, the parties and their legal representatives should bear in mind that technology should be used in order to ensure that document management activities are undertaken efficiently and effectively.

TAR in non-discovery-based countries

In European non-discovery-based countries, there are currently no case law decisions on the use of TAR in administrative and judiciary procedures.

According to European IT experts, TAR is insufficiently used even if e-Discovery is more and more widely used by companies all across Europe:

- many multinational groups based in Europe but active in discovery-based countries might face e-Discovery requests originating from litigation in these countries or investigations carried out by local regulatory authorities (e.g. the French bank BNP Paribas before the US Office of Foreign Assets Control http://www.treasury.gov/press-center/press-releases/Pages/jl2447.aspx).

  In this kind of situation, companies might use TAR, on the one hand, to manage the often massive numbers of documents requested by the authority and make a preselection and, on the other hand, disclose the documents in compliance with their own national rules.

- In fact, many European countries have strict regulations as regard disclosure of data to foreign authorities. French law, for example, provides for a blocking statute, and the French Data protection Authority (CNIL) is very strict in its application of the French Data Protection Act according to which the processing of sensitive personal data is in principle prohibited. TAR may also be a very useful tool to detect personal or privilege data and suppress/redact it from the data provided;

- equally, regulatory authorities like the European Commission may conduct investigations, be it through an RFI or through a dawn raid.

  RFIs often have a very wide scope, which results in a shift of the data analysis burden onto the concerned undertakings. The use of TAR may therefore allow the recipients of an RFI to manage this burden, and process, review and product the requested documents. However, in this case, it would be advisable to submit to the Commission a presentation of the method that the recipient intends to use, and in particular the use of TAR. It will be interesting to follow whether the Commission admits the use of this technology in the response to RFIs.

However, in certain contexts, TAR may present risks that need to be carefully evaluated and limited:

- for example, further to a dawn raid conducted by a regulatory authority or by the European Commission, TAR could seem an appropriate tool to analyze the huge volumes of seized data. However, TAR may "miss" a number of relevant files, due, for example, to a misspell in keywords. Due to this missing factor, TAR be not sufficiently precise to conduct a fully reliable risk assessment. In fact, there is a real risk for the TAR user of unintentionally restraining the scope of the review right from the beginning and to miss responsive documents that the Commission might not miss using more standard methods. This could have a huge impact on the undertaking's defense strategy afterwards.
- before any litigation, companies may conduct internal audits in order to identify potentially non-compliant behavior, and on the basis of the results, decide to settle a case or to apply for leniency in the frame of competition law. For the reasons mentioned above, it would be essential to make sure that the use of TAR does not result in evidence not being identified.

Although the use of TAR in procedures in Europe is still limited compared to other jurisdictions like the US, this possibility is being discussed both in discovery-based and non-discovery based countries. Considering the Irish precedent and the rising interest expressed by European companies for cheaper and quicker tools to manage their ever-growing electronically stored information, TAR use might significantly increase in the future.

However, in certain sensitive contexts, the possible limits of TAR should also be assessed and taken into account.

Chapter 2

Forensics

Forensics can provide evidence as to what users of a device were doing at a certain point in time.

Forensics is one of those words in e-Discovery that is often used by lawyers and vendors without explaining what they mean, which is unfortunate because it has more than one meaning. The two most common meanings refer to either (a) conducting a discovery task in a way that ensures reasonable quality so that the evidence can be used in court; or (b) taking a complete copy of an entire data source -- such as a computer hard drive, thumb drive, phone, or tablet – and then examining it with specific tools and processes.

The first meaning is generally how discovery is conducted in proportion to the needs and context of the case. Preservation, collection, and processing should be conducted in a forensically sound manner such that the party is reasonably confident that data was not lost or corrupted in the process. Put another way, the opposing party and the Court should have reasonable confidence that the relevant information being produced is what it was on the responding party's IT system; that the data has not been corrupted by the discovery process.

The focus of this paper, however, is on the second common meaning of "forensics": the science and art of taking a complete copy of a device, the information a user can easily access and see, and, using special tools, the "unseen" information as well. Thus, forensics has two related but independent steps. First, a "forensic copy" is made –an exact duplicate of the device down to the last bit[1] of data. Second, after restoration and extraction of the "unseen" data, all contents are analyzed by an expert, using forensic technology to determine what evidence exists. Such an investigation may consider deleted data, fragmented data, operating system files, temporary files, the existence of applications or software that may be relevant to analysis, indications of use of external media, deletion timing or patterns, or other obscure data locations and information on the device being examined. This information can provide evidence as to what users of the device may have been doing at a certain point in time and recover electronically stored information ("ESI") that was considered lost. Forensic experts often provide opinions or their inferences about what conduct took place on the device based on the evidence they uncover in their investigations.

Forensics basics

Through the use of industry-standard forensic software (e.g. Encase, Paraben, Cellebrite, Oxygen, FTK, or many others), a trained and experienced digital forensics investigator can help capture and analyze data and information that is not generally available to the average user. To perform forensic analysis on a device or system, a forensic collection must be performed (or physical disk acquisition) where a bit-by-bit image is acquired.[2] This provides the most fulsome collection method which enables the forensic examiner to fully analyze the entire contents of a device in a controlled environment. Targeted collections, which usually limit the scope and volume of collection, are directed at specific folders, paths, or active data that is potentially relevant to the particular case; such targeted collections will not capture all artifacts (such as deleted data, operating system information, deletion patterns, or historical use of external devices) that would be captured by a full forensic collection and as required for a forensic investigation.

Authentication is the verification step that validates if the copy used to perform the investigation is an exact copy of the source by comparing the checksums of the copy and the original.

Analysis is the science and art of investigating the data, both active and unallocated to identify facts that are pertinent to whatever is in dispute. As described in more detail below, this can include recovering deleted files, understanding user behavior, uncovering intrusions or file movement. These investigations often involve artifacts such as temporary files, lnk files, deleted files in unallocated or slack space,[3] logs, and volatile data that lives only in system memory, as well as network and transaction logs are examples of data artifacts that are necessary for these types of investigations.

1 Bit is short for "binary digit," the smallest unit of computer data. A bit consists of either 0 or 1. There are eight bits in a byte.

2 For full forensic investigations, it is most common to make mirror images (the highest standard), or full logical images (one step down from mirror images). Because unallocated space is constantly being overwritten, to get the most out of the collection, it is best to do so as soon as possible or to disallow use of the device until the mirror image is taken. Devices that optimize their memory storage quickly, like servers, overwrite their unallocated space quickly and make forensic analysis of such space for deleted or fragmentary files of little value. On the other hand, server logs or the search for other information may be fruitful.

3 Unused space at the end of a file, or unused clusters of a disk that often contain deleted information from previous uses and have not been removed or completely overwritten from the physical disk or the file block.

Forensics terminology

As its own area of study, digital forensics has its own terms of art. The most common ones describe the types of data typically found on data sources, and the manner of making copies of data sources.

Types of Data on a Hard Drive or Data Source

For forensic purposes, data is described by how the operating system, data management system, or other hierarchy system formats, manages, or ignores data.

- **Active Data:** Files actively managed by the Operating System and mostly accessible to the user.
- **Hidden Data:** Files and locations actively managed by the Operating System but not visible to the user.
- **Deleted (but managed) data:** Files marked as deleted, but still actively managed by the Operating System.
- **Slack data:** Non-file data stored in an allocated area.
- **Unallocated space:** Space that may contain fully recoverable files, file fragments, formatted but unwritten space, or unformatted space.

Active Data: This is information that is normally accessible to the user and the operating system. It consists of files that are managed, available and intact. Active Data is a combination of user data, application files, the operating system, including active processes running in memory, and related logs and configuration files (such as the directory that points to user files).

Unallocated Space: The area of computer media, such as a hard drive, that does not contain normally accessible data. Unallocated space is usually the result of a file being deleted, or portions of a drive not yet used. When a file is deleted, it is typically not actually erased, but is simply ignored and is no longer accessible through normal means. The space that the file occupies is marked as being available to be overwritten, and the space that it occupied becomes unallocated space, *i.e.*, space on the drive that can be reused to store new information. Until portions of the unallocated space are used for new data storage, in some instances, the old data remains and can be fully or partially retrieved using forensic techniques. Often times, an entire partition of data, (*e.g.*, a user's former operating system or data profile) that was formatted can be recovered from unallocated space.

Within the unallocated space can exist nothing (the area has not been used), deleted but fully recoverable files, or fragments of deleted, but only partially recoverable, files.

Types of Data Collections

Methods of copying data vary from single files, to bulk copies of files, to bit-copies of the entire device. While the scope of these copies varies, the techniques of copying them in a "forensics manner" usually rely on specialized tools and prior training to ensure integrity in the process.

"Targeted Collection": A copy of a select number of user files and, or operating system artifacts.

"Logical Collection" or "Active Collection": A copy of all the active data (or all the active files that contain user content) on a data source. This ignores unallocated space.

Live Memory Acquisition or "RAM Collection": A live collection of processes and programs running in memory and/or a collection of targeted memory objects - system files where a system state is temporarily stored (e.g. memory dump or hibernation file). This method of collection is often used in particular situations such as Virus/Malware or network intrusion analysis needs.

"Forensic image" or "bit-by-bit image" or "image" or "mirror image": An exact copy of a data source that includes all the active data, unallocated space, and slack space. Generally, this type of collection is preferred in order to conduct a comprehensive forensic analysis, but is not always (a) possible, (b) practical, or (c) necessary. For example, a bit-image of a database is challenging to make, may interfere with the database's operations, and, due to regular maintenance, may be of marginal value beyond a logical copy. In the instance of a database, for example, if a "forensic analysis" is needed, something less than a bit-by-bit image could be analyzed, such as more easily available audit trails or log data.

Things you can learn from forensics

Recover Deleted Data

Because "delete" does not always mean complete eradication from existence, Deleted Data can sometimes be recovered through forensics. Recovered data may include entire files or only portions, depending on how much activity has occurred on the device since deletion. Importantly, the more a device is used in the ordinary course, the more unallocated space will be overwritten, which will lower the chance to recover Deleted Data. This is true across multiple devices and systems (computers, mobile devices, databases etc). Therefore, the expected success of using forensics to recover Deleted Data drops depending on when the data was deleted.

User Activity
Through analysis of device artifacts, lawyers can learn about a user's activity and how they interacted with their devices. Examples could include information on a user's internet search history, last system login and activity dates, most recently used files, network connections, evidence of wiping utilities, or destruction of evidence.

Another example is a timeline of user events that took place. For example, one could pinpoint the day an employee stole sensitive trade secrets by downloading it on a USB drive, or when a user synced data to cloud storage, such as Dropbox, to use for competitive gain.

Other examples could include reporting on the substance of deleted emails, images, and text messages, as well as social media artifacts that would show dates, times, and GPS locations that photos were taken on an iPhone, or Wi-Fi hotspots used on certain days of the week by that user as they traveled throughout the day or week.

File Movement
The creation, editing, viewing, movement, storage, copying, and sharing of files can be traced though a combination of data traces residing in individual files, logs, shortcuts, links, temporary files, operating system registries, file tables, indexes, deleted files, trashcans, and other locations sprinkled throughout a central computer hard drive or other storage device.

Intrusion Detection
Network and malware analysis are other forms of examination that can show data breaches, network intrusions, and what type of information is being monitored, stolen, or destroyed, and what geographical locations from which points of access derive. Proactive forensic solutions can also be deployed across networks in order to learn about a threat profile and help minimize intrusions.

The United States perspective

In the United States, forensic copying and analysis is certainly the exception in civil litigation. Courts must resolve two common disputes regarding forensics: (1) should it happen at all (i.e., is it reasonable); and (2) how should the forensic investigation occur.

When is forensics appropriate?

First, like most discovery, the question of whether forensics should occur is based on whether the court reasonably believes that the evidence expected to be found is worth the expense and intrusion into likely irrelevant information. Generally, a digital forensic investigation is uncommon and is typically beyond the scope of most preservation or discovery exercises. "Absent a showing of special need and relevance, a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual data or documents." The Sedona Conference, Principle 9; *see also* Seventh Circuit Pilot Project Principle 2.04(d) ("The following categories of ESI generally are not discoverable in most cases, and if any party intends to request the preservation or production of these categories, then that intention should be discussed at the meet and confer or as soon thereafter as practicable: (1) "deleted," "slack," "fragmented," or "unallocated" data on hard drives; (2) random access memory (RAM) or other ephemeral data; (3) on-line access data such as temporary internet files, history, cache, cookies, etc."[4] Requests for forensic information or for a forensic examination may be within the scope of ESI discovery contemplated by Federal Rule of Civil Procedure 34(a)(1)(A), but such requests are subject to the proportionality and relevancy limitations under Rule 26(b)(1) and (2)(C)(iii).[5] Thus, forensics is meant for only those cases where those areas of a computer that a user cannot usually access and use (e.g., operating system files, tracking files, residual images, deleted copies, traces of viewing, copying, printing, deleting, etc.) are expected to have unique, relevant material information, and is typically only allowed when there is suspicion that the data has been tampered with, when the user has sought to conceal their activity, or when a party has not complied with its preservation or other discovery obligations.[6] Courts are more likely to grant a request for a

4 *See also* Principle 9 and Commentary ("Deleted information may at one time have been a 'useful' document generated in the ordinary course of business that had value to the organization, although that value may have expired. However, this historic fact alone does not justify the retrieval and review of deleted information. Case law indicates that only exceptional cases turn on 'deleted' or 'discarded' information (whether paper or electronic). Employees and organizations properly and routinely delete or destroy documents and electronically stored information that no longer have business value, so long as the information was not subject to regulatory, investigatory, or litigation preservation obligations when deleted or destroyed.").

5 *See, e.g., Nola Spice Designs, LLC v. Haydel Enters., Inc.*, Civil Action No. 12-2515, 2013 WL 3974535, at *2 (E.D. La. Aug. 2, 2013); *Balboa Threadworks, Inc. v.. Stucky,* No. 05–1157, 2006 WL 763668, at *3 (D. Kan. March 24, 2006) (courts "have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in the lawsuit are unduly vague or unsubstantiated in nature.").

6 *See ,e.g., Procaps S.A. v. Patheon Inc.*, No. 12-24356-CIV, 2014 WL 800468, at *3 (S.D. Fla. Feb. 28, 2014) (ordering forensic analysis by a neutral, third party forensic examiner when the responding party failed to implement a formal litigation hold and permitted its personnel to self-collect); *Koosharem Corp. v. Spec Personnel, LLC*, Civ. A. No. 6:08–583–HFF–WMC, 2008 WL 4458864, at *2 (D.S.C. Sept. 29, 2008) (allowing forensic analysis on computers because of failure to produce documents).

forensic production if the requesting party has offered to pay the additional expense of such production.[7] Determining whether a forensic collection and production are reasonable and proportional in a particular litigation is a fact-specific inquiry that will vary from case to case.[8]

Inspections vs. Productions.

Generally speaking, to conduct a forensic analysis of a data source (e.g., a computer or mobile device), you either need a bit-by-bit copy or the actual device, which are essentially equivalent. This means that a forensic examination will grant access to the requesting party and their experts to a significant amount of irrelevant information and, potentially even privileged information. As such, a forensic examination usually requires an inspection of a portion of the responding party's IT systems, at least constructively. Because of these issues, there is a general resistance to inspections.[9] The amendments to the Federal Rules of Civil Procedure effective December 1, 2015, specifically address this by providing that "[t]he responding party may state that it will produce copies of documents or of electronically stored information instead of permitting inspection."[10]

Not uncommonly, a requesting party will seek to have their own forensic expert investigate their opponent's devices because they do not know exactly what is on the device, and many argue that a bit-by-bit sector examination is necessary to provide the best and most accurate opinion. Responding parties, not surprisingly, object to such requests because the devices will undoubtedly contain not only a great deal of irrelevant information to which the responding party is not entitled, but possible privileged and other information that is protected from discovery.[11] However, there are instances where an opponent might be entitled to a forensic analysis of a party's devices, such as instances where there is a good-faith allegation that the user of the device(s) purposefully hid information or was intentionally conducting nefarious activities.[12]

Forensic Protocols

As discussed above, if the parties are required or have agreed to allow for a forensic inspection, one of the biggest issues in doing forensics is who is going to do it to protect access to privileged or irrelevant data.

Tension can arise between both parties if no protocol is in place. The responding party can get upset if the requesting party gains access to irrelevant and/or privileged information. On the other hand, many forensic examinations are triggered because of concerns about the honesty or competence of the responding party to fulfill their discovery obligations. Defining the role of the forensics expert and the protocol put into place to achieve consensus on the approach from preserving to production should be the goal, but is not easily achieved. Protecting the producing party's confidential material while identifying only data that is responsive must be reasonable with the requesting party's goal of finding all relevant evidence. Often protocols are misunderstood or do not elaborate on important issues. The most important thing is to freeze the data and make sure that it cannot be corrupted and then develop a thoughtful process to analyze it.

If the parties cannot agree to an appropriate protocol, then a neutral third party or court-appointed forensic examiner may be the best path (paid by both parties). Appointment of the proper neutral expert should require the development and execution of detailed protocols to provide assurance to all parties. The expert should be competent and able to develop this initial protocol, which should cover the following areas:

- The communication protocol between parties regarding the results.
- To what data sources, data locations, and types the examiner should have access.
- How to address the level of transparency to test and validate the producing party's claims of privilege or irrelevance.

7 *B&B Hardware, Inc. v. Fastenal Co.*, No. 4:10CV00317 BRW/JTR, 2011 WL 2115546 (E.D. Ark. May 25, 2011).

8 *See* Seventh Circuit Pilot Program Principle 2.04(a), 2.04(b) (Scope of Preservation)

9 *See, e.g., In re Ford Motor Co.*, 345 F.3d 1315 (11th Cir. 2003); *Bethea v. Comcast*, 218 F.R.D. 328, 329-30 (D.D.C. 2003) (finding that speculation and conjecture did not demonstrate the relevance of any information on the defendants' hard drives and did not warrant inspection of hard drives containing "voluminous information relating to many topics other than plaintiff's employment discrimination claim").

10 Fed. R. Civ. P. 34(b)(2)(B).

11 *Genworth Fin. Wealth Mgmt, Inc. V. McCullan*, 267 F.R.D. 443, 446 (D. Conn. 2010) (any right to forensic information "is counterbalanced by a responding party's confidentiality or privacy interests" (citing Notes of Advisory Committee on 2006 Amendments)); *Bradfield v. Mid-Continent Cas. Co.*, No. 5:13–cv–222–Oc–10PRL, 2014 WL 4626864 (M.D. Fla. Sept. 15, 2014) (denying request to forensically inspect computer system because of privacy and burden concerns where plaintiff merely thought there was additional information to be found on the computer).

12 *See, e.g., Weatherford U.S., LP, v. Innis*, No. 4:09–cv–061, 2011 WL 2174045 (D.N.D. June 2, 2011) (requiring defendant to give a plaintiff-chosen expert access to its computer systems because of plaintiff's claims that materials had been accessed despite defendant's claims to the contrary); *Ferron v. Search Cactus, L.L.C.*, No. 2:06-CV-327, 2008 WL 1902499 (S.D. Ohio April 28, 2008) (ordering a mirror image of computer system hard drives, but allowing plaintiff's forensic expert to remove "Plaintiff's personal confidential information that could not reasonably lead to the discovery of information relevant to this litigation" prior to providing to defendants).

- Whether the requesting party should receive access to the producing party's search terms or search methodology.

Whether a court-appointed or neutral expert conducts the examination, the protocol should detail the scope of examination by providing clear direction to the examiner. For example, in running searches for relevant keywords and documents, it should be clear and concise on proper search syntax. A common mistake is for parties to agree upon a search protocol without conferring with the consulting expert on the process and technique, resulting in partial search results due to syntax issues that had already been agreed to.

Considerations

Once a party has agreed to produce certain forensic information or once a Court has determined that forensics are appropriate in a given matter, parties should ensure that the forensic expert is using acceptable and reliable tools and that such expert can communicate effectively any findings to the court.

Acceptable & Reliable Tools

Once parties decide or the court orders a forensic production or investigation, acceptable and reliable tools must be chosen. Forensic technology is traditionally a generation behind the current devices available to consumers today, which means a full device/disk acquisition is not always possible. However, most types of user-created content and forensic artifacts are, in most cases, accessible even if this is the case. Forensic examiners that are designated should be familiar and trained on a variety of forensic tools and techniques and should have many technologies available as part of their toolkit.

Determining what is an acceptable level of competency in this field and the proper acceptance of evidence from experts varies widely across jurisdictions. Fortunately, the growing recognition of international standards, certifications, training programs, and forensic tools are addressing this need. Current independent forensic examiner certifications (vendor-neutral) more common today include the following: CCE (Certified Computer Examiner), CHFI (Computer Hacking Forensic Investigator), CFCE (Certified Forensic Computer Examiner), GCFA & GCFE (SANS Organization Computer Examiner Accreditations), as well as tool specific certifications such as ACE (AccessData) and EnCE (Guidance Software), which hold ample weight in the industry. These certifications require that candidates possess the necessary skills, knowledge, and ability to conduct formal incident investigations and advanced incident handling and analysis, and many experts should fit into this category.

Facts and Inferences

In addition, forensic examiners must be able to communicate findings to the courts in a clear and understandable way and should clearly distinguish between facts, inferences, and opinions. More importantly, the expert needs to be able to use facts to support conclusions. Human interference is prone to error, therefore, investigators should understand the relation between the inferred conclusions and the facts that support those conclusions.

The Canadian perspective

In Canada, most cases do not require or involve the use of forensic technology. Parties generally take steps to preserve and collect information without the need for mirror images of devices to be made or analyzed. However, there are certain cases where the use of forensic technology is almost a certainty and others, where it will depend on the facts at issue as to whether a forensic analysis will be required. Parties are often able to agree on the imaging of devices and servers when the circumstances warrant, but when the courts weigh in on this issue, the discussion almost always comes down to proportionality and a balancing of the cost, intrusiveness and expansion of the documentary discovery on the one hand, versus the need to obtain relevant information and ensure parties comply with their discovery obligations on the other.

At the outset of litigation or an investigation which may involve issues of data being deleted or not easily accessed, a forensic image of the sources of electronic information should be considered. If there is evidence that a party has engaged in the destruction or hiding of electronic information (e.g. allegations of fraud, conspiracy or misappropriation of confidential information), it would be prudent for the party investigating or seeking relief to ensure that mirror images are taken of all relevant devices and servers. In some situations, it may also be prudent for a party whose conduct is impugned to agree to a forensic image at the outset so as to avoid findings that they have obstructed the investigation or not satisfied their discovery obligations. Agreeing to take an image does not necessarily mean that the image will be produced for analysis by others. Having the image available can go a long way to establishing cooperation.

Establishing the need for a forensic image in litigation does require something more than simply asserting that more documents must exist. Without evidence that a party has attempted to avoid their discovery obligations, courts are reluctant to order that forensic images be taken. For example, in *The Catalyst Group Inc. v. Moyse*,[13] the Ontario Superior Court of Justice refused to order that servers and devices be imaged where the moving party had not produced sufficient evidence that the responding party had "engaged in any destruction of evidence or in any conduct 'designed to hide or delete electronic or other information.'"[14] Thus, even though issues of misappropriation of confidential information were engaged in that case, the court did not consider there was enough evidence to warrant an imaging and review of servers and electronic devices.

If, however, proper forensic steps are not taken or sufficient documentary production is not made, courts will intervene and order that devices be produced for imaging. In *Honour v. Canada (Attorney General)*,[15] the court ordered that a computer hard drive be produced for forensic imaging after it became clear that the party had not made adequate production of documents and had not provided a sufficient explanation of the steps taken to try to recover information. It was apparent in that case that documents had been deleted or overwritten and so the court ordered that an independent forensic analysis of the mirror image of the hard drive be performed.

Images should be taken to the appropriate standard or there may be issues with the use or reliability of the image later in the process. Many parties insist upon an independent third party specialized in forensics taking the image, but that additional expense is not always necessary provided the party who is taking the image can provide sufficient details so that everyone is satisfied the image has been properly secured. Both sides do need to engage someone who can determine whether the image has been taken properly. Not every computer service provider has the ability to take a forensic image and it is important to consult a recognized expert in the area to ensure it is done correctly.

Once an image has been secured, the parties need to engage in a discussion to determine the appropriate review. Issues to be agreed upon include the devices or servers to be searched, the search terms to be applied and a protocol for reviewing documents for privilege. All steps taken should be properly documented. Again, if parties can establish that they have made reasonable, proportionate steps to review the information and have done so responsibly, they generally can avoid orders for additional review. Courts are sympathetic to concerns of costs and are willing to hold parties back from the "turn over every stone" approach unless there is some reason it is warranted.

It is important that the need for forensic imaging be considered at the outset of any conflict or investigation. Securing data on a timely basis can be critical in some cases and it is often in the interest of all parties to try to reach an agreement to do so. However, in most cases, courts are not willing to require forensic analysis without sufficient evidence of wrongdoing or data destruction.

The European perspective

In Europe, regulatory authorities are entitled and even encouraged to use forensic techniques. However, in practice they tend to use them rather sparingly and not always to their full extent. This is also the case with parties before a civil court in the frame of litigation.

This limited use is probably partly due to cost reasons and partly to insufficient knowledge of the advantages and results that forensics allow. There is no doubt that, as the mentalities evolve, forensic techniques will be increasingly used in all fields.

There is also a trend where organizations that have both a global and/or local presence are obtaining an in-house forensic approach when dealing with the need to forensically capture data from their IT environment. This is where an organization builds an in-house forensics team that deals with the need to capture sensitive data prior to being viewed / analyzed by any external entity.

The rare use of forensics before civil courts...

A distinction needs to be made between discovery countries and non-discovery countries.

Discovery countries

In European discovery countries like the United Kingdom, issues linked to the use of forensics in the frame of civil discoveries are close to those encountered in the U.S.

13 2015, ONSC 4388 (CanLII).

14 Ibid at para 57.

15 2008 BCSC 851 (CanLII), leave to appeal denied 2008 BCCA (CanLII).

In the UK, guidelines on electronic evidence disclosure are provided by the Practice Direction 31(b) of the Civil Procedure Rules[16], according to which one of the key considerations is the reasonableness of any search from which a disclosure is made.

Thus, for example, when the disclosure concerns electronic documents, "a party requesting disclosure of additional metadata[17] or forensic image copies of disclosed documents (for example in relation to a dispute concerning authenticity) must demonstrate that the relevance and materiality of the requested metadata justify the cost and burden of producing that metadata."[18]

Therefore, in the UK, the parties will need to consider whether or not metadata is likely to be relevant to the issues at stake and, if so, determine more specifically what types of metadata are most likely to be relevant.

Non-discovery countries

Although in civil law countries such as Germany or France, there are no discovery procedures similar to those in the UK/US, issues linked to forensics may occur before civil jurisdictions.

In France, for example, Article 145 of the Code of civil procedure[19] provides for an action ***in futurum*** which entitles a party to ask the judge, under certain conditions, to order the disclosure of documents before any proceeding.

Once a procedure has been initiated, a party may also seek a production order from the judge concerning documents known to be in the possession or control of another party. To succeed, a request for production of documents must be rather specific ("fishing expeditions" are prohibited). Thus, according to the rationale of this procedure, the use of forensics seems unlikely in most cases. However, in some specific situations, the use of forensics might be effective and appropriate, for example in case of doubt regarding the authenticity of a document, when deleted documents need to be recovered or when the activity logs may help to resolve a dispute.

Furthermore, it is becoming increasingly common that companies active in non-discovery countries (especially – but not only – multinationals) have to face discovery requests ordered by a common law court in the frame of a litigation.

In order to respond to this request, the company concerned would have to cope with some peculiar provisions in force in most of civil law countries such as:

- Reinforced data protection rules that regulate potential transfers of data abroad;[20]
- Labour law, especially provisions which protect employee's right to privacy; and
- Specific issues related to the application of so-called "blocking statutes".[21]

For a party placed in any of these situations, the use of forensic techniques might be useful in order to ensure better control of the data at stake.

... as well as by regulatory authorities

In Europe, law enforcement agencies, and in particular the European Commission, have extensive investigative powers, which may result in *de facto* discovery, in which procedural rules are less clearly defined than in a discovery-based country.

One of these powers consists in their faculty to use forensics in the frame of an investigation.

In the competition law area, the European Competition Network, which is a forum for discussion and cooperation within European competition authorities, has issued a recommendation on the power to collect digital evidence[22] according to which: "all Authorities should have effective and efficient powers to gather digital evidence, including evidence obtained forensically, through inspections of business and/or nonbusiness premises, requests for information and other investigative tools. To that end, the Authorities should have the power to gather all information in digital form related

16 Civil Procedure Rules, Practice Direction 31B – Disclosure of electronic documents (last updated on 22 October 2013).

17 i.e. beyond the metadata that naturally accompanies documents disclosed in native format.

18 Civil Procedure Rules, Practice Direction 31B – Disclosure of electronic documents, paragraph 28.

19 This article provides that "if there is a legitimate reason to preserve or to establish, before any legal process, the evidence of the facts upon which the resolution of the dispute depends, legally permissible preparatory inquiries may be ordered at the request of any interested party, by way of a petition or by way of a summary procedure."

20 In France for example, Deliberation n°2009-474 of 23 July 2009 makes recommendations regarding the transfer of personal data in the frame of US discovery proceedings, e.g.: data collected as part of a discovery procedure must be adequate, relevant and not excessive compared to the purposes for which the treatment is implemented.

21 National "blocking statutes" prohibit any national party from disclosing commercial information whether originating from the country concerned or elsewhere in foreign litigation, absent a national court order.
See for example the German Federal Data Protection Act promulgated on 14 January 2003 or the French Blocking Statute (Law 68-678 of 26 July 1968).

22 ECN recommendation on the power to collect digital evidence, including by forensic means, of 9 December 2013.

to the business(es) under investigation, irrespective of the medium on which it is stored and the technological evolution of the storage media. The Authorities should also have powers to gather digital information by taking digital copies, including forensic images, of the data held and/or through the seizure of storage media."

In practice, most of the European competition authorities have such powers. For example, the European Commission's Inspectors are expressly entitled to "make use of their own dedicated software and/or hardware (Forensic IT tools)" as well as "copy, search and recover data whilst respecting the integrity of the undertakings' systems and data" to search the IT-environment of a company.[23]

However, although law enforcement agencies use forensic software in virtually all inspections, they do not systematically use all the functions of forensics for obvious costs/efficiencies reasons. Like before civil courts, one of the main reasons to use it could be if, in the frame of an investigation, an authority has doubts on the authenticity of one or several document(s) seized on company premises; or if the agency believes that some potentially interesting files have been deleted before its investigation.

One difficulty that is faced when undertaking a forensic capture/collection exercise, is where organizations introduce encryption into their IT environment for either software or hardware (laptop, desktop, etc).

In conclusion, the decision to use forensics has to be based on an analysis of the proportionality of the measure compared to its purpose. Companies must nevertheless keep in mind that most of law enforcement agencies have the power to use forensics in the frame of their investigations, and shall not hesitate to use forensics to realize an internal audit, should they have doubts about their compliance with European regulations in some specific areas.

However, given the multiple advantages of forensic techniques, it seems unavoidable that the next years will see a significant development of their use both in civil procedures and regulatory investigations.

The Australian perspective

When is forensics appropriate?

Like the United States, forensic copying and analysis is an exception in civil litigation.

In most Australian jurisdictions, parties are obliged to discover relevant documents (including electronic documents and meta data) that are in the party's possession, custody or power. In recognition of the increasing volume of ESI, some Australian jurisdictions have taken steps to reduce the burden of discovery. In particular, this paper will discuss the Federal Court's approach to discovery.

The Federal Court controls the discovery process. The Court will only order discovery if it will facilitate the just resolution of a proceeding quickly, inexpensively and efficiently. In determining whether to make any discovery order, the Court will consider the resources and circumstances of the parties, the likely benefit and costs of discovery, and whether that cost is proportionate to the nature and complexity of the proceeding.

A party is only required to undertake a reasonable search for discoverable documents, which among other things, requires an assessment of the ease and cost of retrieving a document, and the significance of any document likely to be found.

Before the Court orders that discovery be given by exchanging documents in electronic format, it expects the parties to have discussed and agreed on a practical and cost-effective discovery plan that takes into consideration the issues in dispute and the likely number, nature and significance of the electronic documents that might be discovered.[24] The parties should consider whether a forensic collection is necessary during the plan's preparation.

The Federal Court also has the power to order that the requesting party pay in advance for some or all of the estimated costs of discovery, or to require the requesting party to give security for the costs of discovery. Therefore, if a requesting party seeks the other party to undertake a forensic collection which may involve significant cost but only produce information or documents of dubious relevance and little probative value, the Court may order the requesting party to bear the cost of discovery.

23 Explanatory note on Commission inspections pursuant to Article 20(4) of Council Regulation N° 1/2003.

24 A similar limitation also applies to discovery in Victorian courts. Observations to similar effect have also been made in other jurisdictions, including WA and NSW.

Where it is evident that a party has not complied with their discovery obligations and has deleted discoverable documents, the court may order that party to produce all devices for forensic analysis.[25] In *Moody Kiddell & Partners*, it was alleged that the respondents had copied the applicant's client list and used the confidential information to establish their own brokerage service. When it became evident that the respondent had deleted relevant discoverable material, the applicant's forensic expert was given access to the respondent's computers, servers and storage devices. The analysis revealed that the respondent had downloaded the applicant's client list and that file destruction software had been installed on his home and new business computers. As a result, the Court struck out part of the respondents' defense for abuse of process. In a later judgment on the matter of costs, the court ordered the respondents to indemnify the applicants for the costs of and incidental to the forensic analysis and strike out application.[26]

Inspection vs production

The Federal Court has ordered parties to provide access to an entire database where it was considered important to receive data in an electronic form and in the same level of detail as the original source data.[27] However in another case, an application to access an entire database was rejected partly on the basis that the database would give access to every facet of the respondent's business.[28]

Australian courts also have the power to order a respondent to permit other persons (a search party) to enter premises, search for documents or material, inspect, copy documents and remove property from the respondent's premises.[29] This form of order is termed a search order or historically an *Anton Piller* order. Search orders are often sought in cases of copyright infringement and misuse of confidential information and intellectual property.

The object of a search order is to preserve important evidence pending the hearing and determination of the applicant's claim. The search party includes the applicant's legal representatives and usually independent computer experts. The search party is supervised by independent legal representatives.

The terms of the order typically permit the independent computer expert or the independent lawyer to remove computer hard drives from the respondent's premises, either for safekeeping or to copy its contents.

In recognition of the highly invasive nature of a search order, the Court will only grant a search order if certain conditions are satisfied, such as sufficient evidence that the respondent possesses important evidentiary material, and there is a real possibility that the respondent might destroy the material or make it unavailable for use. The Court also requires the applicant and the members of the search party to give undertakings to the Court regarding their conduct.

Forensic protocols

Where documents are to be forensically collected and examined, as in the United States, the parties should endeavor to agree on a protocol to protect access to and use of privileged, confidential and/or irrelevant data.

If the parties cannot agree on the protocol, either the parties or the Court may engage an expert or advisor to assist with resolving any issues that have arisen when attempting to develop an electronic document management protocol.

25 *In Moody Kiddell & Partners Pty Ltd v Arkell* [2013] FCA 1066 the respondent deleted numerous relevant emails, despite having been warned of his obligation not to destroy relevant documents. The applicant's forensic expert was given access to the respondent's computers, servers and storage devices.

26 *Moody Kiddell &Partners Pty Ltd v Arkell* [2013] FCA 1225

27 *Jarra Creek Central Packing Shed Pty Ltd v Amcor Limited* [2009] FCA 60

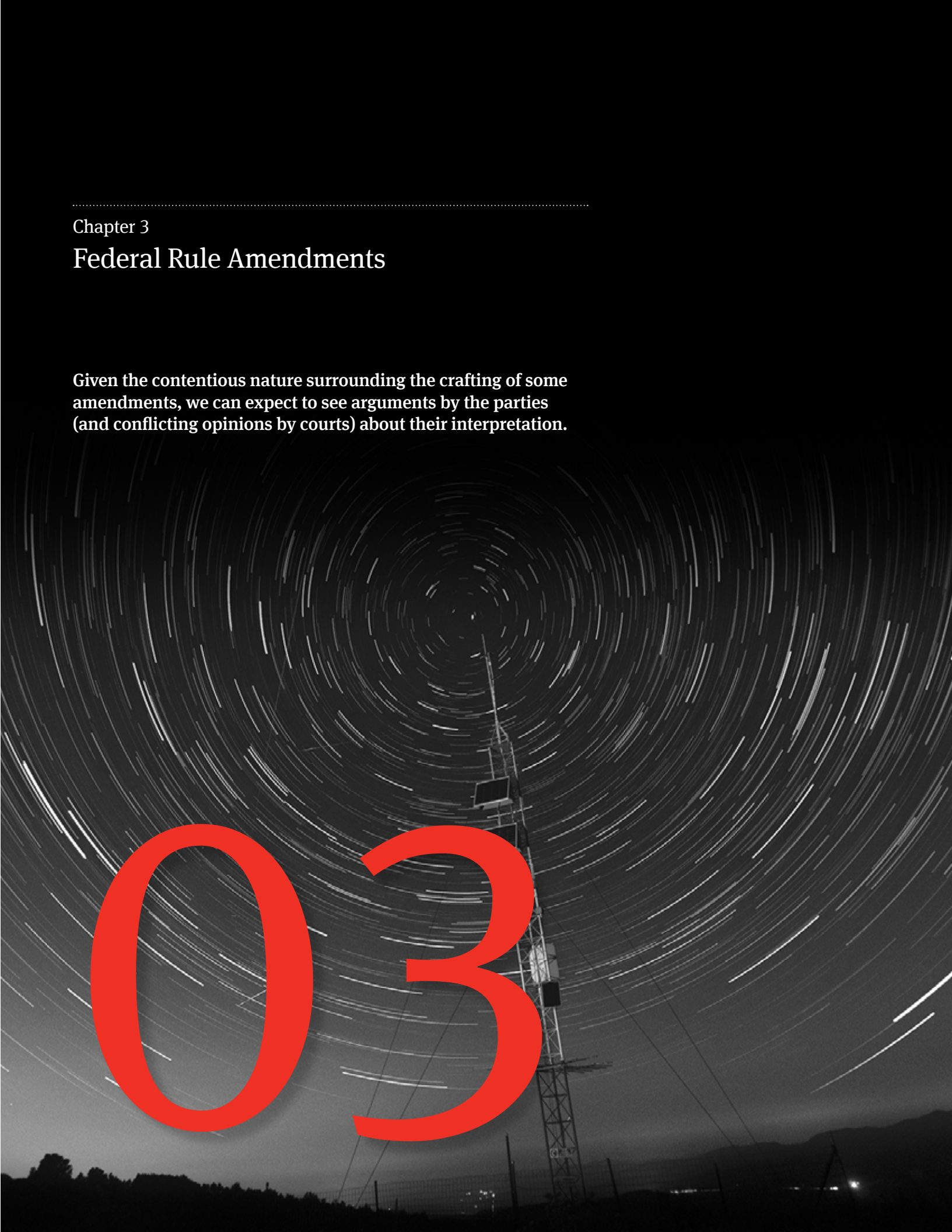
28 *Kyocera Mita Australia Pty Ltd v Mitronics Corporation Pty Ltd* [2005] FCA 242

29 Each Australian jurisdiction has attempted to harmonise their rules and procedures regarding the making of search orders.

Chapter 3

Federal Rule Amendments

Given the contentious nature surrounding the crafting of some amendments, we can expect to see arguments by the parties (and conflicting opinions by courts) about their interpretation.



03

On December 1, 2015, a number of important discovery-related amendments to the Federal Rules of Civil Procedure took effect. The amendments reflect an attempt to resolve conflicting authority among the Federal District Courts and clarify areas of confusion that have arisen as the bench and bar have matured in their approach to electronic discovery. The amendments are best understood as a refinement to the amendments adopted in 2006, which directly addressed the discovery of electronically stored information ("ESI") for the first time.

Although the amendments are a clear step forward in defining the obligations of courts and litigants in Federal Court, the full implication of these amendments will not be understood until courts have had opportunity to interpret and apply them. Given the contentious nature surrounding the crafting of some amendments, we can expect to see arguments by the parties (and conflicting opinions by courts) about their interpretation, particularly with respect to the amendments to Rules 26(b)(1) and 37(e).

This article discusses the four most prominent amendments to the discovery-related Rules: 1, 26, 34, and 37. Below we list the amended rules, highlighting the updated text, followed by a brief synopsis. A comprehensive listing of the amendments to the Rules and Advisory Committee notes may be found at the Supreme Court's website.

Expanding the general duties of parties to employ the rules

Rule 1. Scope and purpose

These rules govern the procedure in all civil actions and proceedings in the United States district courts, except as stated in Rule 81. They should be construed ~~and~~, administered, **and employed by the court and the parties** to secure the just, speedy, and inexpensive determination of every action and proceeding.

Synopsis:
Although Rule 1 has been amended to require parties, not just the district courts, to employ the Rules to "secure the just, speedy, and inexpensive determination of every action and proceeding," what is perhaps more important is what is not in the amended Rule 1. The Committee considered inserting "cooperation" into the rule, but decided not to do so. Instead, the Committee stated in the advisory notes that "[m]ost lawyers and parties cooperate to achieve these ends" and that "[e]ffective advocacy is consistent with – and indeed depends upon – cooperative and proportional use of procedure." While the Committee Note emphasizes that this Rule change does not create a new or independent source of sanctions, at least one judge has already pushed back on this by stating that the court has inherent authority to sanction parties for failing to cooperate.

Scope of discovery and cost shifting

Rule 26. Duty to disclose; General provisions governing discovery

* * * * *

(b) Discovery scope and limits.

(1) Scope in General. Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged 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. Information within this scope of discovery need not be admissible in evidence to be discoverable. ~~—including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated~~

~~to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(C).~~

(2) Limitations on frequency and extent.

* * * * *

(C) When required. On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:

* * * * *

(iii) the burden or expense of proposed discovery <u>is outside the scope permitted by Rule 26(b)(1)</u> ~~outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.~~

* * * * *

(c) Protective orders.

(1) In general. A party or any person from whom discovery is sought may move for a protective order in the court where the action is pending — or as an alternative on matters relating to a deposition, in the court for the district where the deposition will be taken. The motion must include a certification that the movant has in good faith conferred or attempted to confer with other affected parties in an effort to resolve the dispute without court action. The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following:

* * * * *

(B) specifying terms, including time and place <u>or the allocation of expenses</u>, for the disclosure or discovery;

Synopsis of amendments to Rule 26(b)(1):
The amendments to Rule 26(b)(1) are intended to prevent parties from broadening the scope of discovery to "the subject matter of the case" upon a showing of good cause. This was the old standard that was changed in the early 1980s to "relevant to claims and defenses" but some courts had failed to recognize that the updated rule narrowed discovery and often applied the overbroad "subject matter" standard as the baseline for discovery. The amendments intentionally narrow the scope of discovery to stop courts from using this broader formulation.

The amendment makes clear that if a document is relevant and within the scope of discovery, the mere fact that it may be inadmissible does not bar its production. The Advisory Committee note to Rule 26 remarks that the "reasonably calculated" phrase in the current Rule 26(b)(1) was removed because "[t]he phrase has been used by some, incorrectly, to define the scope of discovery" and "has continued to create problems[.]"

Proportionality is a key element of discovery and limits the scope of discovery even beyond relevance. The amendment moves the mandatory proportionality factors from the current 26(b)(2)(C)(iii) and to the forefront of 26(b)(1). The Advisory Committee note to Rule 26 explains that this was done to "restore" the proportionality factors to their original place in defining the scope of discovery. This change reinforces the Rule 26(g) obligation of the parties to consider these factors in making discovery requests, responses, or objections. Importantly, the amended Rule 26(b)(1) includes a new factor for courts to take into consideration when determining proportionality of requests, "the parties' relative access to relevant information." While this change was made to emphasize the importance of proportionality in discovery and does not change the need for considering the marginal benefit and cost of discovery, by incorporating proportionality in the definition of scope, the amendment explicitly incorporates proportionality into preservation. Documents that are not discoverable need not be preserved. Parties preserving unilaterally, however, should not be overly aggressive in relying on proportionality to not preserve documents until the case law becomes more settled.

Reflecting the Advisory Committee's commitment to the application of proportionality throughout the discovery tools, Rules 30(a)(2) and 31(a)(2) have been amended to require the Court to grant leave to conduct oral and written depositions "to the extent consistent with Rule 26(b)(1) and (2)." Rule 33(a)(1) has been amended to allow a court to grant leave to a party to serve more than 25 interrogatories "to the extent consistent with Rule 26(b)(1) and (2)." Similarly, "court must allow additional time" beyond the seven-hour time limit for oral depositions "consistent with Rule 26(b)(1) and (2)" if needed.

Synopsis of amendments to Rule 26(c)
The amended Rule 26(c)(1)(B) provides responding parties another tool to keep discovery proportionate and reasonable: cost shifting. A party may now ask the court to include in protective orders "allocation of expenses." The amendment abrogates the minority of cases holding that courts may not shift discovery costs unless the underlying data is not reasonably accessible. This provides an opportunity for producing parties to argue that if marginal or barely proportionate discovery is going to be allowed, it should be paid for by the requesting party to ensure that they only push for discovery where they believe the value outweighs the cost. The Advisory Notes are clear, however, that this language was not meant to change the general rule that producers pay for their discovery productions.

Changing how parties respond to discovery requests

Rule 34. Producing documents, electronically stored information, and tangible things, or entering onto land, for inspection and other purposes

* * * * *

(b) Procedure.

* * * * *

(2) Responses and objections.

(A) Time to respond. The party to whom the request is directed must respond in writing within 30 days after being served or — if the request was delivered under Rule 26(d)(2) — within 30 days after the parties' first Rule 26(f) conference. A shorter or longer time may be stipulated to under Rule 29 or be ordered by the court.

(B) Responding to each item. For each item or category, the response must either state that inspection and related activities will be permitted as requested or state an objection with specificity the grounds for objecting to the request, including the reasons. The responding party may state that it will produce copies of documents or of electronically stored information instead of permitting inspection. The production must then be completed no later than the time for inspection specified in the request or another reasonable time specified in the response.

(C) Objections. An objection must state whether any responsive materials are being withheld on the basis of that objection. An objection to part of a request must specify the part and permit inspection of the rest.

Synopsis:
Quickening the Ability to Serve Document Requests
The amendments to Rule 34 may significantly change how parties respond to discovery requests and produce documents. First, the amended Rule 34(b)(2)(A) works in tandem with the amended Rule 26(d)(2), which now permits service of discovery requests before a Rule 26(f) conference in certain cases and considers such early requests "to have been served at the first Rule 26(f) conference" regardless of when the request was sent or delivered. The purpose of these two rules is to encourage requesting parties to serve their requests before 26(f) conferences so that the parties can better meet and confer about the scope of the discovery. However, one of the other practical effects of this rule is that parties may respond to discovery very quickly, potentially even before the Rule 16 scheduling conference.

Specificity and choice to produce
The first amendment two amendments to Rule 34(b)(2)(B) simply memorialize the existing law in most federal courts. Requiring a party to state "with specificity the grounds for objecting" to a request tracks Rule 33(b)(4)'s current requirement that parties must state objections to interrogatories with specificity and many courts had incorporated it into Rule 34. See, e.g., *Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 359-60 (D. Md. 2008). Second, the amended Rule 34(b)(2)(B) allows a party to specify whether it will allow inspection of ESI or produce copies of ESI. While it is helpful to have this explicitly stated in the Rules, most courts had found that a party can choose to produce or permit an inspection and that a court could not force an inspection over objection without good cause. See, e.g., *In re Ford Motor Co.*, 345 F.3d 1315, 1316-17 (11th Cir. 2003).

Informing requesting party when productions will be complete
The amendment to Rule 34(b)(2)(B), however, may have the biggest impact on the behavior of responding parties and require them to state the reasonable period of time in which they will complete their production. At the time a party responds to requests it may be hard to know when

productions will be substantially complete. For example, the scope of discovery is likely still being negotiated and a party may still be investigating the volume of information that may be at issue. Moreover, while the Advisory Committee understood that productions are often made on a "rolling" basis, the Advisory Committee notes counsel that "[w]hen it is necessary to make the production in stages the response should specify the beginning and end dates of the production." In light of this amendment and the accompanying note, therefore, counsel should be careful not to rely on open-ended promises to produce information on a rolling basis. In addition, it is unclear what obligation a party has to supplement this date or what will happen to a party who fails to complete its productions by the date it estimates in its response.

Are objections causing the responding party to withhold documents?

Finally, the biggest philosophical change to Rule 34 is included in Rule 34(b)(2)(C), which will now state: "An objection must state whether any responsive materials are being withheld on the basis of that objection." The Advisory Committee comments that this amendment is intended to "end the confusion that frequently arises when a producing party states several objections and still produces information, leaving the requesting party uncertain whether any relevant and responsive information has been withheld on the basis of the objections." The Advisory Committee notes also make an effort to allay concerns that the amendment will place a significant burden on objecting parties to "show their work":

> The producing party does not need to provide a detailed description or log of all documents withheld, but does need to alert other parties to the fact that documents have been withheld and thereby facilitate an informed discussion of the objection. An objection that states the limits that have controlled the search for responsive and relevant materials qualifies as a statement that the materials have been "withheld."

Thus, to comply with this obligation, a responding party could disclose the filters it used to search for responsive information, such as date restrictions, lists of specific data sources, or search terms. This is not without risk as it could generate more scrutiny and motion practice as requesting parties ask to broaden responding parties' searches. In fact, the Rules do not require these specific types of disclosure and parties often wish to avoid such disclosures for the purposes of protecting confidential or privileged information. In such cases, parties should attempt to fashion alternative means of satisfying the amended Rule, such as describing specifically what you are looking for (not "how"), which should provide requesting parties enough information to object if they think the search is too narrow. Until the courts have had time to determine the practical implementation of Rule 34(b)(2)(C), the extent to which litigants will be required to disclose their search and review criteria will remain unclear.

Setting clear standards for spoliation of ESI

Rule 37. Failure to make disclosures or to cooperate in discovery; Sanctions

* * * * *

(e) Failure to provide preserved electronically stored information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system. 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.

Synopsis:

Perhaps the most contentiously disputed amendment, Rule 37(e) has been amended to create a consistent standard for spoliation in all Federal courts. Prior to the amendment, the standards of culpability ranged from mere negligence to recklessness and willful conduct among the various Circuit Courts. As stated in the Advisory Notes, the new Rule

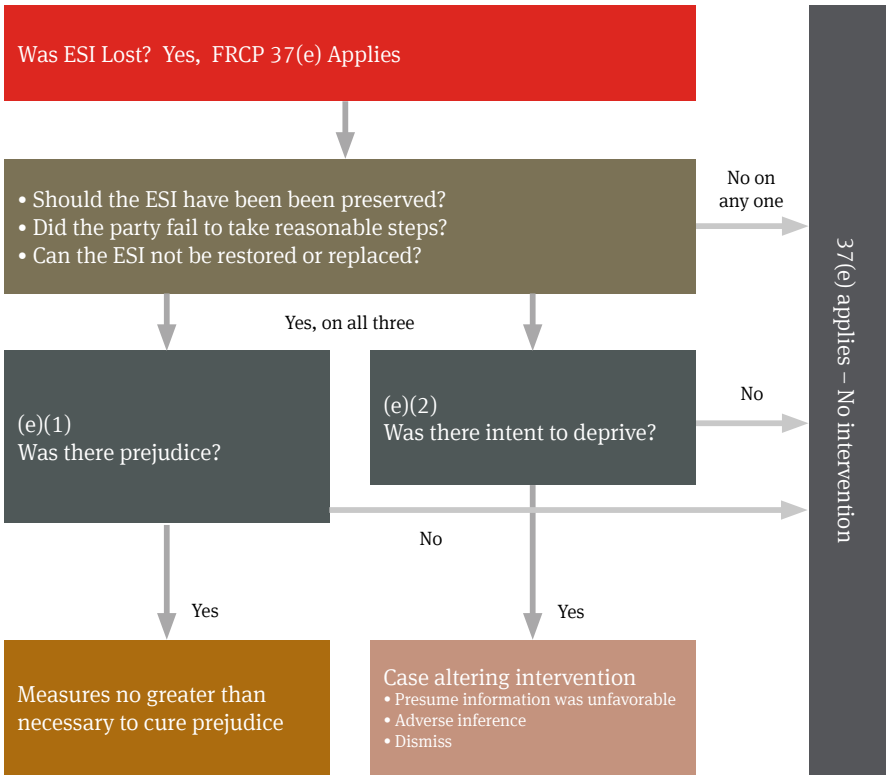
specifically overrules Second Circuit precedent (Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99 (2d Cir. 2002)) that arguably authorized adverse-inference instructions on a finding of negligence or gross negligence.

Now, Rule 37 provides a tiered approach to loss of ESI. First, intervention by the Court under Rule 37(e) is not permitted unless three elements are established: (1) ESI that should have been preserved has been lost, and (2) the party losing the ESI failed to take reasonable steps to preserve it, and (3) the lost ESI cannot be restored or replaced. If these three elements are established, then the court may either: (1) order curative measures if the requesting party is prejudiced by the loss of ESI; or (2) levy the enumerated sanctions if the court determines that the responding party acted with intent to deprive the requesting party of the ESI.

Curative measures can be broad and could include precluding a party from presenting evidence, deeming some facts as having been established, or permitting the parties to present evidence and argument to the jury regarding the loss of information. On the other hand, case altering intervention, including adverse inferences, are only available where a requesting party has lost or destroyed the data with an intent to deprive the requesting party of its use in the litigation (which arguably requires the loss to occur in the current matter and not in a former one). Moreover, the Advisory Notes caution courts about these severe sanctions and emphasize the least draconian sanction should be levied:

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

Thus, while proportionality and prejudice are not explicitly within Rule 37(e)(2), the Advisory Notes make it clear that it is best read with both of these principles in mind. To make new Rule 37(e) more manageable, we have attached a flow chart to help explain the analysis.



Our global offices

*associate office
**alliance

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

NORTON ROSE FULBRIGHT

Law around the world
nortonrosefulbright.com