Anti-Corruption Report
An Acuris company

Dechert LLP

January 6, 2021

ELECTRONIC DISCOVERY

eDiscovery in Multi-Jurisdictional Investigations: Preparing to Play Multi-Level Chess

By Ben Barnett, Karen Coppens, Richard Hodge and Garbis Latifyan, *Dechert*

In recent years, there have been two notable trends in multi-jurisdictional corporate investigations. First, is a marked increase in the extent to which enforcement authorities from multiple jurisdictions are willing – if not eager – to coordinate their investigations and resolutions. Second is a significant increase in enforcement authorities' willingness to use eDiscovery technology and techniques to assist in investigations. These developments, taken together, add additional complexity to designing and implementing an efficient and cost-effective data review for multi-jurisdictional investigations that were already challenging because of national legal differences with respect to criminal statutes, privacy and legal privilege.

Indeed, undertaking a multinational internal corporate investigation has become like playing a multi-level game of chess – one wrong or ill-advised move can have serious consequences in multiple jurisdictions. Fortunately, there are practical solutions to these issues that do not require C-suite executives or senior in-house counsel to become eDiscovery experts.

This article will introduce the key issues and provide a framework so companies and their counsel can appropriately consider and manage these challenges in future investigations. First, we lay out the key steps in the process and then identify six pitfalls to avoid when undertaking an integrated review plan for data in multiple jurisdictions.

For more from Dechert, see "Airbus: The Value of Cooperation" (Mar. 18, 2020).

The Importance of eDiscovery

At the outset, it is important to have a clear and common understanding of what constitutes eDiscovery, particularly for companies and their counsel operating in countries accustomed to magistrate-led investigations. Discovery is a rules-based disclosure process developed in 20th century American jurisprudence, aimed at avoiding trial by ambush and identifying legal claims that do not require factual resolution by a jury. Discovery now exists in both civil and criminal matters in the U.S. and remains largely a counsel-driven process subject to judicial oversight.

The addition of the "e" to discovery to form "eDiscovery" reflects the simple reality that today most data is created, exists and is stored in electronic form. The volume of electronic data disclosed by parties in current matters

and the attendant costs to the parties can be daunting. The significant advancements in using technology to more quickly identify the most relevant data, to avoid wasting time and money reviewing non-relevant information, and to make the disclosure process as effective and efficient possible to reach a timely, reasonable and fact-based resolution are being accepted and endorsed by more authorities in both common law and civil code jurisdictions.

Embrace by Additional Enforcement Authorities

Before the emergence of the global COVID-19 pandemic, there was an accelerating trend of cooperation and coordination among law enforcement authorities conducting multi-jurisdictional criminal investigations. In France, the enactment of Sapin II in 2016 and the pursuit of multiple criminal investigations and prosecutions by the Parquet National Financier (PNF) and *Office central de lutte contre la corruption et les infractions financières et fiscales* (OCLCIFF) vaulted French authorities into a lead role long occupied by the U.S. Department of Justice (DOJ) and the U.K.'s Serious Fraud Office (SFO).

Historically, some enforcement authorities, particularly in E.U. countries, largely rejected the use of eDiscovery technology and techniques developed in the U.S. as too intrusive, costly, burdensome and incompatible with local (civil law) legal traditions. As cooperation and coordination between enforcement authorities continues to increase, that now appears to be changing.

Though many factors (some legislative) contributed to this change, there are three primary drivers:

1. the unmatched efficiency of a well-devised and calibrated eDiscovery process;
2. the massive increase in the volume of business and personal data created every day; and
3. the low cost of data storage including particularly "cloud" storage.

Traditional investigation techniques (*i.e.*, a dawn raid by authorities to seize corporate data) are rendered less effective today because they transfer the burden to authorities to sift through terabytes of irrelevant data to try to find evidence of potential criminal conduct. Instead, authorities are now looking to companies and their counsel to develop and implement innovative solutions to preserve, identify and produce the evidence relevant to an investigation, providing potentially substantial cooperation credit to those companies that succeed in meeting this challenge.

A Patchwork of Data Laws and Regulations

At the same time, an increasing number of governments around the globe have awoken to the enormous importance and value of commercial and personal data. The result has been the enactment of a patchwork of country-specific laws seeking to control and regulate such data, including data on the internet (hence the rise of the so-called splinternet) or hosted by cloud service providers (CSPs). These laws go well beyond traditional blocking statutes that barred the export of certain sensitive or commercially valuable data.

See "How the New French Guidance on Deferred Prosecution Eligibility Affects Settlement Negotiations" (Oct. 30, 2019).

Planning and Deploying an eDiscovery Strategy

Global enforcement authorities now may well expect more sophisticated approaches that target and focus the data review to advance the investigation or to demonstrate cooperation particularly in the context of deferred prosecution settlements. Recent widely publicized corporate resolutions confirm this trend. If companies consider these issues carefully at the outset, and involve the right team in the discussions, there is a far greater likelihood that the data review will meet their business and litigation objectives and satisfy relevant external legal standards and expectations, while saving substantial time and money.

Each investigation is unique, and the eDiscovery process should be designed and structured to best meet the company's objectives and the authorities' expectations. Companies should be mindful that "one size does not fit all" particularly when it comes to strategic eDiscovery. Early discussion between the company and its advisers, careful consideration of the relevant issues with the right team, and engagement with relevant authorities where appropriate, will ensure a smoother process – ultimately paving the way for a stouter defence or swifter resolution.

Companies need to consider at the outset of a project what laws, regulations or practices potentially govern retention or review of corporate data, including whether that data can legally be transmitted or transferred to another country for attorney review and analysis. The review planning phase should equally pay attention to the investigative standards and expectations of major global enforcement authorities including the DOJ, the SFO and the PNF namely that:

- evidence should be preserved, collected and disclosed promptly and comprehensively; and
- a sound, thorough and well-documented process of preservation, collection and production is critical for the credibility of an investigation.

Multinational companies are likely to have extremely complex and diverse IT architectures, with data stored in many ways and locations. Documented processes for preserving, collecting and reviewing data, and for responding to regulatory or enforcement enquiries will ensure the company is best placed to respond quickly and not be caught on the "back foot," or face liability or the loss of credibility for failing to account for and preserve potentially relevant data.

Broadly speaking, eDiscovery work falls into four phases:

- data preservation;
- data collection;
- data processing and review; and
- productions of relevant material or evidence.

Data Preservation

Potentially relevant evidence normally falls into one of three categories: hard copy or paper documents, structured data (databases), or unstructured electronic data. The evidence may be held by employees or in central repositories such as archives, company vaults, or on servers and back-up systems. Determining how company employees create, store and archive data is a critical first step,

which may necessitate the assistance and involvement of the company's subject matter experts such as the IT team and archivists to ensure implementation of a successful process. Failure to preserve data or, worse, the inadvertent destruction of data can expose a company to serious adverse scrutiny and suspicion – and potential criminal sanctions if the destruction of data was deliberate.

To avoid these outcomes, in-house counsel should issue a "document retention notice" (DRN) to relevant individual employees at the commencement of an investigation. An effective DRN should address three key questions:

1. what data is relevant;
2. which employees are likely to possess potentially relevant data; and
3. what actions should or should not be taken to preserve potentially relevant evidence.

Widely distributed DRNs may not be appropriate in cases where document collections need to be conducted covertly to avoid tipping off employees who may have engaged in potential criminal conduct. In such circumstances, companies must proceed cautiously to avoid privacy infringement or running afoul other data restrictions.

Data Collection

The collection process for multi-jurisdictional investigations may be a substantial and potentially disruptive exercise if not managed properly. Before launching the process, the investigation team should pause, consider the objectives and challenges of the exercise, and devise a sensible and defensible collection plan.

Data Protection Considerations

Data protection legal advice should be sought prior to the collection process, and communications with concerned employees should be carefully managed to avoid any potential challenges by employees for alleged infringement of their privacy rights.

Consider Hiring Forensic Experts

Expert forensic IT and data collection vendors should be consulted to undertake the collection process. While the fees and costs in instructing external vendors for forensic collections can be significant, involving third-party subject-matter experts ensures that the independence of the process is preserved. Moreover, doing so will help establish the credibility of the collection process, allow a company to accurately and credibly respond to questions or concerns from regulatory or enforcement authorities, and avoid company personnel bearing direct responsibility for errors that may occur during the collection process.

Identify Relevant Custodians

Identifying employees who may hold potentially relevant data is a critical step: if too narrow, the company may face criticism for failing to preserve and collect relevant material, but an overly broad, "boiling-the-ocean" approach could cause significant disruption to the business, and unnecessarily cause loss of time and money. The process is an evolving one and should be kept under review throughout the course of the investigation as it and the understanding of counsel evolves.

A collection interview should be carried out with each relevant individual immediately prior to collection of their data. Interviews can be conducted remotely to comply with pandemic travel restrictions or reduce travel expenses. The interview should be conducted by the company's external legal advisers to ensure the necessary independence, though in some circumstances where there are employee sensitivities or concerns it may be appropriate and useful for in-house counsel to participate in the interview.

See "Remote Forensic Data Collection Steps Into the Spotlight" (Jul. 22, 2020).

Formulating a Strategy

As with the collection stage, it is important to discuss and clearly define a company's overall objectives in analysing data before launching a review.

Define the Scope

The review area in particular is one where "one size does not fit all." For instance, a company may wish to get to the bottom of an allegation as quickly as possible, which will require a targeted, focused and prioritised review model. On the other hand, a company may wish to make substantial productions to a relevant regulatory or enforcement authority to demonstrate cooperation and the absence of any actual criminal conduct, which will require a far broader approach to review and analysis. In reality, it is unlikely that any single review method will be sufficient for a disclosure project of any significant size or complexity.

Invariably, the data review stage is the most time-consuming and costly part of the eDiscovery process. Taking the time to consider and settle on agreed strategy up front is one of the most effective cost-saving steps a company can take.

Whichever process is deployed, it is important to spend sufficient time planning the process to ensure the review strategy is effective and fit-for-purpose. That said, the company and its counsel should continue to evaluate its approach as the investigation unfolds and be prepared to make appropriate changes, as necessary. Far from demonstrating a lack of confidence in the process, remaining flexible will ensure the company remains focused on the end objectives in the most timely, efficient and defensible manner.

Involving Regulators

Where an investigation involves external reporting, early engagement with the relevant regulator or enforcement authority will help ensure sufficient "buy-in" is obtained, and any concerns regarding the proposed review methodology are raised and resolved. As with the preservation and collection processes, the company should document its approach and be ready to defend should it face later scrutiny. Particularly in the context of a DPA, companies need to anticipate that the authorities will want to understand the review process and have a chance to review and evaluate the quality of productions.

Data Review

There are three primary review methods to review and analyse (or code) the collected data. Choosing the right approach (or approaches) in an investigation is critical.

Linear Review

A linear review involves a document-by-document review to determine responsiveness. The advantage of this method is that all documents will be considered for relevance. The main disadvantage is the significant time needed to complete the review. Where electronic data is involved, even small investigations will typically involve thousands of emails or other documents.

Search Terms

Another option is to narrow the scope of a linear review through the application of tested keyword "search terms" to identify documents which are more likely to be relevant. The value of this process is limited by the quality of the search terms. For instance, where a particularly relevant exchange is written in code or slang, it may omit the keywords and therefore fall outside the scope of the review. The quality of the search terms will have a direct impact on the quality of review and poor search terms will result in the review of irrelevant or inconsequential files.

Predictive Coding

Predictive coding, or "technology-assisted review" (TAR), involves algorithm-based tools designed to improve the accuracy of identifying and predicting whether a document is likely to be relevant. TAR is conceptual in approach: in this sense, it goes "beyond" search terms, although it is limited by the suitability of the data for complex analytics (for instance some electronic files and scanned hard copy documents cannot be categorized by the TAR algorithm). In a typical TAR exercise, assigned case experts will review a comparatively small "seed" set of documents, applying coding as to whether each document is relevant or not.

As the experts continue to code more sample documents, the computer learns how to more accurately "predict" whether a document is relevant or irrelevant. Once those predictions are demonstrated to be accurate, counsel can defensibly decline to review files that are unlikely to be relevant while using search terms to accelerate the review of documents predicted to be relevant. A second-generation predictive coding tool called "Continuous Active Learning" (CAL) addresses some of the limitations of the TAR model including improved indexing and the ability to have a single integrated CAL and relevance review.

The use of TAR is garnering increasing support, and its deployment can go a long way in appropriately prioritising and focusing a document review, especially where a company has large amounts of potentially relevant data and where traditional review methodologies may be inadequate, outdated or poorly equipped to conduct a review in a way that is comprehensive, targeted and cost-effective. The practice of using TAR is well-advanced in the U.S. and is increasingly supported in other jurisdictions.

Hybrid Approaches

Companies and their counsel are not restricted to using only one of these methods in structuring a data review. A hybrid approach may be preferable, with different categories of documents subject to different review methodologies, or one methodology overlain on another to supplement or prioritise the review. For instance, TAR may be used to whittle down a large document population to material that is more likely to be relevant,

and targeted search terms are then used to prioritise for review the documents which are most likely to be highly relevant. Stratifying a review in this fashion is likely to ensure the company reaches the core issues of a matter as quickly as possible, which may guide the determination of when sufficient review and reporting has been accomplished to successfully resolve a matter.

Production of Relevant Material or Evidence

Productions or presentations following the review process can take multiple forms including presentations of investigative findings, production of documents used in witness interviews, periodic disclosure of highly relevant material, or responses to *ad hoc* requests from the investigating authorities. Where productions are made to regulatory or enforcement authorities, the authorities will likely expect timely and comprehensive delivery, with a documented process they can scrutinise as required.

Companies should also anticipate the need to make internal presentations up to and including the Board of Directors.

For both internal and external productions and presentations the company must adopt a consistent approach. This particularly applies to circumstances where the company intends to withhold relevant material, for instance where it is legally privileged. Companies should be mindful that where they are responding to multiple regulatory or enforcement authority requests across jurisdictions, different laws and regulations may apply. Tailoring a unique production process in such circumstances is a challenge but can be achieved even when dealing simultaneously with authorities operating under different legal regimes.

The production of documents is rarely a one-off exercise, and as such it is important to carefully document the process. If the same data is produced simultaneously to more than one jurisdiction, some adaptation of the production set may be necessary, depending on the requirements in each jurisdiction.

A final practical note of caution – in the framework of multi-authority investigations, it must be anticipated that productions to one authority will likely trigger requests by other authorities. Planning from the outset how to properly manage such requests will save time and money, and avoid sleepless nights.

See "Insights on Negotiating With the DOJ: The Filip Factors and Compliance Presentations" (Aug. 5, 2020).

Six Pitfalls to Avoid

Multi-jurisdictional or cross-border investigations implicate a number of challenges and complexities in designing and deploying a defensible eDiscovery process, which, if not thoughtfully planned, managed and monitored, could entail a number of risks or potential pitfalls for the company. Significant missteps can be fatal to the integrity of the investigation and potentially impact a company's reputation, operations and finances. In a worst-case scenario, the company or its employees may face potential criminal liability for the destruction of relevant evidence. What follows is a list of the six most common pitfalls to avoid when undertaking an integrated review plan for data in multiple jurisdictions.

1) Carrying Out an Incomplete Exercise

Perhaps the biggest mistake a company can make in an eDiscovery process is failing to preserve, collect, review or produce relevant material. Failures can arise at any stage of the process and may seriously impact confidence in and the integrity of the process or final product.

It is necessary to ensure that the scope of the exercise is appropriately defined at the outset and modified as appropriate as the investigation progresses to ensure that potentially relevant data is identified and preserved.

2) Losing Legal Privilege

Many jurisdictions permit the withholding of otherwise relevant materials because of legal privilege or protection. Ensuring that such material is withheld from disclosure is an important consideration. Inadvertent or compelled disclosure in one jurisdiction may have implications for the protection of the same material in other jurisdictions.

See "Dispelling Myths About When Attorney-Client Privilege Applies to Communications With In-House Counsel" (Sep. 20, 2017).

3) Data Privacy

Data privacy laws, including the E.U.-wide General Data Protection Regulation (GDPR) and related criminal and employment provisions apply to the retrieval, processing and use of data during an eDiscovery exercise as well as to the transfer of data abroad, with different regimes for transfers inside the E.U. and EEA or to third countries.

The use of company electronic devices (laptops, mobile phones, etc.) and networks by employees for private, non-company purposes may be tolerated or protected. Such protection may be overridden in cases of ongoing criminal investigations, or if the employer has received court authorisation to access the material, but the local jurisdiction position will need to be checked and confirmed in every case.

See "GDPR Enforcement Lessons and New ICO Guidance on COVID-19" (Apr. 29, 2020).

4) Blocking Statute Provisions

Regulatory and enforcement authorities normally obtain responsive documents through international treaties, mutual legal assistance requests (MLATs) and informal information channels.

However, companies responding to production requests based on the exercise of legal process or to support self-reporting or self-disclosure are bound to comply with applicable legal restrictions on the external transmission of certain potentially relevant evidence. These include "blocking statutes" in some countries, such as France and China.

For a discussion of the role France's blocking statute took in the Airbus settlement, see "Airbus Case Marks a Milestone in International Anti-Corruption Cooperation"

5) Security Restrictions

Certain companies, by virtue of their activities or contracts with governments or the public sector, may possess information which implicates a country's national security and defence. Preservation, protection and proper management of such classified or national security data is crucial.

See the Anti-Corruption Report's two-part series on China's State Secrets Law: "A Primer for Anti-Corruption Practitioners (Part One)" (Jun. 29, 2016); and "Six Things to Consider When Engaging in Internal Investigations in China (Part Two)" (Jul. 13, 2016).

6) Highly Regulated Industries

Highly regulated sectors are subject to specific restrictions in the way they organise, operate and dispose of data. This is certainly the case in the financial services, healthcare and consumer protection sectors. Clients must work with their counsel to make certain that sector specific regulations are followed through the eDiscovery process.

Conclusion

Companies should ensure that they pause, plan and reflect on the most appropriate strategy to deploy from the outset. No two investigations are entirely alike and developing a tailored approach will save time and cost for the company in the long run.

A well-structured and reliable process of eDiscovery will provide a company with an effective route to the bottom of an allegation or dispute, and ensure it has a defensible and respectable position before relevant courts, regulators or enforcement authorities.

Finally, an effective eDiscovery process can provide support for a company seeking resolution via a deferred prosecution agreement, representing a significant factor in assessing the company's cooperation credit and, when done properly, result in a massive reduction of the financial penalty underlying that resolution.

Ben Barnett
Partner
+1 215 994 2887
ben.barnett@dechert.com

Ben Barnett is a partner in Dechert's Philadelphia office. His practice focuses on eDiscovery and he has served as lead discovery counsel and strategist in significant civil litigation and criminal investigations for nearly 20 years.

Richard Hodge
Associate
+44 20 7184 7630
richard.hodge@dechert.com

Richard Hodge is an associate in Dechert's London office. He is an experienced white-collar crime and investigations lawyer whose practice focuses on complex multi-agency and cross-border investigations. He has substantial experience in managing complex eDiscovery projects.

Karen Coppens
National Partner
+33 1 57 57 80 57
karen.coppens@dechert.com

Karen Coppens is a national partner based in Dechert's Paris and London offices. Her practice focuses on white-collar crime and investigations. For over a decade she has advised governments, multinational organizations and individuals under investigation by authorities including the Parquet National Financier, French investigating judges, the U.K. Serious Fraud Office and the U.K. National Crime Agency (and their international counterparts). She has substantial experience managing complex multi-jurisdictional investigations and working closely with other advisers.

Garbis Latifyan
Associate
+33 1 57 57 80 80
garbis.latifyan@dechert.com

Garbis Latifyan is an associate in Dechert's Paris office. He is a member of the firm's white collar crime and investigations practice at Dechert, where he focuses on multi-jurisdictional matters.