NEW FRONTIERS

EDISCOVERY 2015

An insight into the global expansion of ediscovery

Key regional insights

The growing role of computer forensics

Uncovering cartels

New technologies in ediscovery

Kroll Ontrack®

Welcome to the inaugural New Frontiers in ediscovery report from Kroll Ontrack

Tim Phillips
tphillips@krollontrack.com

Our report highlights the recent and rapid international expansion of the use of ediscovery techniques and technologies by law firms and their clients as well as the huge progress made in the capabilities of ediscovery itself.

We have witnessed an exponential rise in the use of ediscovery services in countries beyond the traditional homeland markets of the US and UK, where take-up of ediscovery was initially driven by changes to the legal system governing discovery and disclosure in legal proceedings.

Today, ediscovery is becoming an important element of the business and corporate governance landscape, even for countries that do not have an obligation to provide ediscovery under their legal framework.

The important drivers for these countries, including Germany, France, the Netherlands, China and Singapore are more likely to be related to increased scrutiny by regulators, the transparency and compliance agenda, the need to manage mountains of big data and the overriding requirement to reduce legal costs.

As well as breaching additional geographical frontiers, ediscovery technology is also hitting new technology milestones. Predictive coding is now used in almost every new matter we are instructed on in the UK, for example.

Acceptance is growing in the courts of law in the US and Europe and will mean even more demand for clever ediscovery technology in the future.

Finally, demand from our clients all over the world for local expertise and support has driven expansion of our network of data centres and document review teams into more and more locations across the world.

In our report, you can find out more about what's happening with ediscovery in those different regions, why the global financial services sector in particular is applying ediscovery to its own unique market challenges, how organisations are using ediscovery to break up cartels and where technologies are heading to next.

It's an exciting time to be involved in ediscovery and to witness its rapid growth as a problem-solver for everything from regulatory compliance to dealing with dawn raids, and from unbundling legal services to forensic investigations.

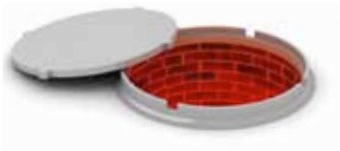
We hope that you enjoy our first report on the international ediscovery marketplace and the many frontiers that it has reached so far.

Tim Phillips
Managing Director
Kroll Ontrack International
Legal Technologies











REGIONAL INSIGHTS

EDISCOVERY TECHNIQUES

Appetite for new technologies IN THE UK

Kroll Ontrack has always been dedicated to pioneering innovation in ediscovery. Over the past few years, predictive coding has been at the forefront of that innovation, and our hard work in developing this technology has been recognised by two awards in 2014: The National Law Journal Award for the most powerful predictive coding technology, and The New York Law Journal award for the best predictive coding solution.

We are delighted to report that some element of predictive coding is now being used in almost every new matter we are instructed on in the UK. Most commonly, this is at the most rudimentary level, where intelligent prioritisation (IP) is used to indicate how important each document is. Clients find that this is particularly useful as they can target the most relevant documents first in a document review and bypass the swathes of non-relevant documents that are often found at the beginning of review exercises, whilst keyword searches are being refined.

Judicial Stamp of Approval

Crucially, IP is not controversial and does not require any judicial stamp of approval which makes lawyers less apprehensive about using it. Full-scale predictive coding – where intelligent categorisation (IC) is employed to make predictions about how each document should be categorised so that lawyers do not have to review each document – does require judicial sanction if it is used during discovery in the course of litigation proceedings. While we do not currently have judicial precedent for this in the UK, we are finding increasing interest in its adoption amongst lawyers and their clients, as many are confident that the UK courts will follow the US courts in allowing its use. For many lawyers, the absence of judicial precedent is attributable only to the fact that a suitable case has not yet come before the courts and therefore it is only a matter of time before IC becomes accepted as routine practice in UK cases.

What has happened recently to add significant impetus to the case for using predictive coding is the judgement in the case of *Irish Bank Resolution Corporation Ltd & ors* v *Quinn & ors*[1]. For the first time, a court closer to home has agreed to the validity of using this technology and the benefits being reaped from it. The ruling addresses major concerns expressed about predictive coding and seeks to sway the sceptics. It unequivocally states that predictive coding will save time and money. The methodology underpinning the use of this technology has been declared sound, as have the benefits of using it.

New Data; New Technology

As the sources of electronic evidence continue to grow it is imperative that those collecting and processing data keep pace with change. We've seen this in recent years with banking litigation casting the net over structured data such as Bloomberg and Reuters data which is produced by companies themselves, and not always in a format which is capable of being easily reviewed. The expertise and data analytics technology required to handle and analyse this structured data exists and is able to unlock valuable insights in cases. Similarly, the technology required to handle complex financial data in relational databases and audio files is becoming increasingly sophisticated and the expertise required to use it is rapidly developing.

Main Users of eDisclosure Technology

The majority of our instructions in the UK come via law firms involved in competition and litigation matters and we try, where possible, to extend these relationships to their corporate clients. This ensures there is a flow of communication between all individuals involved in a project to reduce uncertainty.

Increased regulatory scrutiny from bodies such as the SFO, FCA and CMA have resulted in UK companies developing a closer relationship with edisclosure service providers in order to reduce the risks involved in data harvesting and provide a tighter rein on the costs associated with responding to regulatory demands. Law firms and the companies involved in these matters are also responding by developing inhouse capabilities to collect, process and review data. Companies are becoming increasingly aware not only of the direct costs and risks associated with regulatory scrutiny in the form of data retrieval and possible sanctions, but also the indirect impact on reputation and ultimately share prices.

This more proactive approach to disclosure takes companies into the world of information governance where companies are making greater efforts to get to grips with where data lies within their organisation. The aim is to ensure more targeted and cost effective collections of data and reduced response times. Linked to this are considerations relating to limiting the data produced and kept by organisations with thought being given to how to adjust working practices that lead to the explosion in data volumes and data destruction policies. Typically these issues will touch upon a number of key stakeholders within larger companies (In-house counsel, records management/Information governance professionals, HR, IT, business risk/compliance, data security) who may have conflicting views on best practice but will need to find common ground to work towards an effective data strategy. Going on from this, we are also seeing the emergence of dedicated edisclosure professionals within companies able to steer these groups of individuals and ensure a common approach to data management and ediscovery response across the organisation.

The Legal Landscape

In the UK, the key practice guidance relating to electronic evidence disclosure, as many readers will be aware, is practice direction 31(b) of the Civil Procedure Rules. In essence this mandates that during litigation parties should collaborate as to a proportionate collection/search of electronic evidence prior to the first Case Management Conference. The electronic disclosure questionnaire acts as a guide to those agreeing on an approach to disclosure in litigation and includes the main considerations to consider at this stage.

Since the introduction of this guidance, we have found an increased awareness amongst law firms as to best practice during edisclosure and there is no doubt that lawyers are considering these points earlier in the litigation process where data interrogation is likely to form part of the exercise. As you would expect, as knowledge of the nature of electronic evidence permeates the legal landscape, litigants are increasingly using edisclosure as a point of contention to gain an upper hand on the opposition. The savvy litigant will understand the challenges facing lawyers with respect to locating electronic evidence and will use this to give themselves an advantage during disputes. All litigants, however, are at the mercy of Judges and not all are fully conversant with the intricacies associated with electronic evidence. As far as costs budgeting is concerned, many lawyers are becoming frustrated that the front loading approach to litigation can often be impractical and in some cases are making a stab in the dark when assessing the likely costs of an action. We would advocate, specifically in terms of understanding the costs of edisclosure, using early data assessment tools on a sample of the data at the earliest stage of the case which will give a much firmer idea as to data volumes and scope of the retrieval and review exercise.

Responding to Regulatory Scrutiny

In recent years, we have also witnessed an unprecedented level of regulatory scrutiny and sanctions being imposed on multinational companies; most notoriously in the banking sector. The resource drain on companies brought about by this increased level of regulatory activity has been compounded by the gargantuan levels of electronic data that are now held; which must be organised and inspected appropriately. Often, companies are threatened as much by the cost of complying with the disclosure requirements of regulators, as they are by the prospective sanctions.

As a technology and related services provider, Kroll Ontrack has been inundated with requests to assist our clients throughout the investigation process. The most striking observation we have made is that companies who have a better handle on their data are able to deal with such investigations far more successfully than others.

In light of this, Kroll Ontrack is determined to equip in-house counsel with as much practical knowledge as is necessary so that they may deal with their data in a strategic, cost-effective manner; both on a pre-emptive and after-the-event basis. To that end, in May 2015, working with LegalWeek's Intelligence Unit, we conducted a survey of more than 100 in-house lawyers based in the UK. Our aim was to assess and generate discussion around how companies operating in the UK are responding to a number of trends we had observed in the UK including:

- increased scrutiny by regulators
- more vigilant compliance efforts
- increasing pressure to deal with big data
- changes to the way in which legal services are delivered through the adoption of technology or unbundling of legal services.

Key Findings of In-house Counsel Survey

When considering the main obstacles to providing or reviewing electronically stored documents for legal proceedings, time was the most common problem, followed by costs, logistical challenges when data is scattered in different countries and complying with data protection laws that restrict access to data or transfers across borders.

Some companies have taken a proactive approach to managing their legal risks and are carrying out health checks on their data. They do this by reviewing what they store electronically through internal audits to identify and resolve problems early.

Litigation and arbitration arising in the UK was the most common cause for companies to have to process and search electronically stored data for proceedings, with 48% of respondents having taken this route. This was closely followed by internal investigations, overseas litigation, investigations by UK authorities, mergers and acquisitions activity and foreign regulatory probes.

Survey respondents look to a variety of integrated cost control means to reduce legal spend related to big data management in legal proceedings, with most carrying out work internally using their own software and solutions, followed by relying on external law firms to implement cost saving mechanisms and using technology provided by a vendor.

Companies are most likely to outsource legal document review to a third party other than a law firm when there are short time scales or large volumes.

A full briefing on the results of the survey is available at www.ediscovery.com/cms/pdf/KOT_LR_e-discovery_research.pdf.

by Chris Chapman
Legal Technologies Manager, Kroll Ontrack
chris.chapman@krollontrack.com

1 [2015] IEHC 175

The German experience

For a civil law system, with no tradition of discovery, Germany is rapidly emerging as the largest European ediscovery market after the UK. A combination of regulatory zeal, recent EU developments to introduce disclosure for follow on damages actions and continued high sensitivity around data privacy has attracted investment to develop the full range of ediscovery services in-country.

In the Perview of Regulators

The Bundeskartellamt is an independent competition authority whose task is to protect competition in Germany and it is renowned as one of the most active authorities in Europe. Investigations into cartels and market abuse are very high on the authority's agenda, while merger control seems to be the main order of business for the regulator. In 2015, the Bundeskartellamt lists dozens of current merger control proceedings in its perview, with a significant number of those cases in second phase examination proceedings. A key feature of these proceedings is the request for internal documents, which causes respondents to perform classic ediscovery searches, document review and disclosure in a much shorter timeframe than a litigation disclosure exercise in England and Wales. The timetable for responding to such requests is almost completely divorced from any regard for how much work is involved, meaning that parties are forced to continually manage expectations around delivery, through regular monitoring and reporting of progress and a system of rolling productions, to establish the flow of evidence.

Export-oriented German companies with international trade relations and Austrian companies with a strong presence in Central and Eastern European countries have a high risk of getting involved in international cartel investigations. Therefore, they become more and more interested in being prepared for such incidents, especially when they do business in overseas markets, where they may have less visibility of employee behavior and more so in critical markets such as Russia and China. In these circumstances, the data protection and data security challenges can be more stringent than in cases involving domestic data. When data is not allowed to leave a country companies are increasingly looking for agile ediscovery solutions to keep their data behind their own firewall. In countries where the movement of goods (i.e. processing equipment) is restricted, it is of heightened importance that the solutions for securing and searching data are readily available on a laptop, rather than a mobile server.

Opening the Door to Discovery

The EU Directive on Antitrust Damages Actions was finally adopted by the Council on 10 November 2014. This means that Germany, like all member states of the European Union is working towards implementing this in German law. Article 15 of the Directive states that "evidence is an important element for bringing actions for damages for infringement of Union or national competition law". In "order to ensure equality of arms", both claimants and defendants in actions for damages are afforded the right to obtain the disclosure of evidence. Disclosure is a novelty in German law, since German litigation does not involve discovery. It is anticipated that this new requirement will help make it easier to claim for damages and with this, it is thought that German companies will need more guidance in navigating the ediscovery seas.

Market Study on Ediscovery in Germany

Such an increase in ediscovery activity may help German companies to regard it as a normal business function. This year, Kroll Ontrack published a market study into ediscovery experience in Germany and found, among other things, that many companies are reluctant to admit to having had an ediscovery experience, for it tends to suggest that the company has had an embarrassing problem. Nevertheless ediscovery is prevalent in Germany and as it expands into the German disputes management system, it is likely to become more commonplace and more accepted. This expectation has certainly been the impetus for ediscovery companies opening data centres and document review service centres in Germany this year. For a full copy of our report on the market study please see our website www.ediscovery.com/cms/pdf/Ediscovery_in_Germany_Short.pdf.

Looking Ahead

Costs and speed will continue playing a significant role in the future, when companies have to carry out internal investigations or have to disclose evidence for an authority. Technology assisted review has become an integral part of ediscovery projects in Germany by helping clients to meet tough deadlines and to save costs. Looking at the increasing number of international ediscovery projects taking place Managed Document Review services will play an important role in guaranteeing a consistent level of quality

German data protection law is one of the strictest worldwide. While some companies have tolerated data being hosted outside of Germany, the arrival of local processing facilities has come as a huge relief. The NSA scandal remains uppermost in the minds of the German public, meaning that, ediscovery suppliers must offer their clients local technical solutions and consultancy from local people, who speak the same language and have the same cultural background.

by Helmut Sauro
Senior Consultant, Kroll Ontrack
hsauro@krollontrack.com

THE FRENCH OVERVIEW

France is a civil law country where there is no formal discovery. However, ediscovery is used in various situations where Electronically Stored Information (ESI) must be collected and searched.

Competition matters

Ediscovery and computer forensics tools and techniques are now commonly used by the European Commission and national competition authorities to conduct dawn raids and seize companies' electronic data. Therefore, companies and their lawyers tend to use a similar approach by using ediscovery platforms to review seized data after a dawn raid or to carry out proactive audits in search of business risks. In France, some law firms still use relatively old methods of reviewing documents by copying the data onto their computers or servers to perform a manual review with Microsoft Outlook and Office software, or even by printing them. Although this approach is cheaper and may be acceptable in smaller matters, it's impractical because cases often have tens of gigabytes of data.

Data volumes can be particularly large as the French Competition Authority (*Autorité de la Concurrence*) takes the specific approach of copying entire mailboxes without restriction. It considers a mailbox as a single indivisible electronic file which therefore must be seized wholly, to maintain its integrity. This approach is controversial since a lot of irrelevant and privileged emails are also seized. The French competition watchdog recently implemented a new sealed envelope procedure to appease critics. Now, companies subject to a dawn raid can ask for privileged documents to be removed before the seizure. In this context, it can be useful to get an early assessment of what has been seized in order to quickly identify privileged materials but also discover what has happened in a case and develop a strategy for responding.

Global regulatory investigation

There have been some recent cases which have illustrated that large French companies face increasing risk from US Authorities such as the Departement of Justice (DOJ), the Securities and Exchange Commission (SEC) or the Office of Foreign Asset Control (OFAC). The risk is particularly difficult to manage due to the cultural and legal gap between French companies and common law systems. Dealing with US regulators usually requires full cooperation from companies which have to identify and disclose every relevant document. This is a very unusual approach for a French company and French lawyers. In addition, logistical and technical challenges usually arise because of the volume and diversity of data, deleted files, and legacy systems, not to mention data protection issues.

Privacy and data protection developments

In France, the handling of ESI within an ediscovery project is subject to privacy and data protection rules which are known to be quite strict. Nevertheless, some recent developments are noteworthy.

One should remember that unless it is marked as personal, data stored on computers used by employees is presumed to be professional and can therefore be accessed by employers in an employees' absence. This rule has recently been extended to personal USB sticks[1] and external hard drives[2] connected to professional computers. This development definitely gives companies more ability to control their data.

When it comes to the transfer of data abroad in foreign proceedings, French companies often face a dilemma whether to adhere to the Blocking Statute[3] or to comply with their disclosure obligation. However, recent decisions from both American[4] and British courts[5] show how weak the Blocking Statute argument is because of the lack of local enforcement by French courts. Moreover, the current debate which aims to better protect French companies' business secrets also brings some uncertainty on the future of the Blocking Statute. From an ediscovery perspective, local data processing and hosting solutions are often required in order to best comply with data protection rules. In its 2009 deliberation[6], the French Data Protection Authority (CNIL) recommends among other things that data should be filtered on a local basis i.e. in the country where the personal data is located.

In a new digitalized and globalized world, French corporates need to adopt new reflexes and strategies in order to adapt themselves to the new litigation and regulatory game. The role of ediscovery is definitely growing at the same time as a compliance culture is developing.

by Thomas Sely
Business Development Manager, Electronic Evidence, Kroll Ontrack
tsely@krollontrack.com

1 French Supreme Court, employment section, Feb 12, 2013, n°11-28649
2 Versailles Court of Appeal, Jan 15, 2014, n°12/01664
3 Law n°68-678, 26 July 1968, modified by Law n°80-538, July 16, 1980
4 Activision Blizzard Inc. Stockholder Litig., 86 A.3d 531 (Del. Ch. 2014)
5 National Grid Electricity Transmission PLC v ABB & ors [2013] EWHC 822 (Ch), April 11, 2013
6 Deliberation No. 2009-474 of 23 July 2009 concerning recommendations for the transfer of personal data in the context of American court proceedings known as "Discovery"

Securing electronic data in the Netherlands

Electronic discovery in the Netherlands refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in an internal or regulatory investigation, civil or criminal legal case.

Electronic devices and communications have greatly simplified the ability to conduct business in the Netherlands. It has at the same time introduced risk and added to the sheer volume of data that companies need to manage and protect and to the volume of evidence that needs to be preserved and reviewed. The key to addressing these issues and handling electronic evidence requests successfully is to take a proactive stance to managing electronically stored information and to incorporate new technologies and methods into the handling of evidence in Dutch cases.

The Spotlight in the Netherlands

Recently the spotlight in the Netherlands has been on internal and external investigations. There are numerous drivers for launching an internal investigation. These include misconduct in employment, data theft, suspicion of internal fraud, or indications of possible corrupt payments. In any investigation, the first step should be to establish what actually happened, so the company can tailor an appropriate approach towards obtaining answers and completing the investigation quickly and thoroughly.

At this stage it is important to engage with a varied network of experts to achieve the results required. The network may comprise of external legal counsel, IT professionals, digital forensic and ediscovery experts. Regardless of the type of investigation, the collection of documents can be from custodians located in the Netherlands or scattered around the world. The varied documents (emails, financial records, or expense accounts, for example), may be written in different languages. Relevant information might also be stored in different media sources. Given these challenging parameters, the best course of action is to get a sense of the potential scope of the data that needs to be collected and the extent of the review required as quickly as possible. Legal teams in the Netherlands often look to outsource the first level document review to a provider of document review services.

Increasingly Active Regulators

In the world of external investigations regulatory and enforcement agencies may lead *dawn raids* (unannounced inspections) to obtain evidence. The purpose of a raid is to investigate a specific complaint or concern a business is not complying with the competition rules or sector specific regulations. Dawn raids are part of the range of enforcement measures of the Dutch authorities including the Netherlands Authority for Consumers and Markets (ACM). The ACM are becoming increasingly active and are carrying out strategic dawn raids on businesses to check on compliance. Last year, the ACM carried out dawn raids at the premises of an unknown number of providers of energy auctions. The dawn raids were a direct consequence of signals received by the ACM that the energy auctions and energy suppliers had made price-fixing arrangements.

Following the creation of the ACM over a year ago, the Netherlands has also recently introduced a Streamlining Act to harmonise its enforcement powers. The Act extends the ACM's powers to conduct a raid not only in competition enforcement, but now also to address concerns in telecoms and for consumer protection. Consequently a rise in the number of dawn raids is expected. The key reforms covered in the Act include raising the worldwide threshold for a merger notification from €113 million to €150 million (which is likely to lead to a slight reduction in merger notifications), and limiting the rights of former employees to remain silent regarding the behaviour of their former company (although they can still refuse to speak about their own conduct). Such new powers should be warning enough to prompt companies to review how long they keep electronically stored information and how well positioned they are to retrieve what they need when the authorities launch investigations.

In May this year, the Dutch Senate passed a Bill on the Notification of data leaks. This law imposes an obligation on "data controllers" in the Netherlands to notify the Dutch Data Protection Authority (CBP) and affected individuals when there is a breach. The law may require data controllers to update agreements and their data processor to account for breach notice obligations. It also increases the fines capable of being issued in terms of the Dutch Data Protection Act (DPA) to up to €810,000 or 10% of the company's net annual turnover. Both data controllers and data processors may be subject to the fines. This law makes it important for companies to understand their digital landscapes and their obligation to keep data secure, retain it for no longer than necessary and have the ability to investigate breaches.

Proactive Audits are Critical

Given the Dutch regulators' ongoing focus on compliance, targeted due diligence and proactive audits are critical for companies in the Netherlands. Such audits can be geared to test the company's general response to a potential surprise inspection and they can be used to make employees better aware of what to expect from what is generally acknowledged to be a chaotic and highly stressful experience.

The use of regular internal audits is also an opportunity to develop expertise in the same emerging technologies used by regulatory authorities for data mining. These technologies include machine assisted review, communication analytics, concept searching and topic grouping to aid early case assessment and immediately prioritise data for analysis. In a live investigation, such expertise could be the marginal gain required to get ahead of other parties and the regulators themselves.

A Strategic Weapon

Ediscovery in the Netherlands goes far beyond mere technology. It is an important strategic weapon in the search for evidence and the drive towards compliance. It seems sure that in the Netherlands, companies and authorities alike will have the development of their ediscovery capabilities high on their agenda in 2015.

by Tina Shah
Legal Consultant, Kroll Ontrack
tshah@krollontrack.com

Pinning down trends in America

American ediscovery is ever-changing, as exhibited both by ongoing trends in the industry and court opinions. In 2014, the hottest ediscovery topics ranged from the use of technology assisted review in litigation, to the preservation of texts and social media, to the increased need for cybersecurity. Furthermore, with the amended Federal Rules of Civil Procedure poised to go into effect later this year, American ediscovery law is in a constant state of change.

The Hottest Topic is Predictive Coding

The *hottest* topic in American ediscovery in the last 12 months was the expanded use of predictive coding (sometimes called technology assisted review or TAR). According to a Kroll Ontrack survey of law firms and corporations, over 40% of law firms and corporations used predictive coding on at least one matter in 2014. Practitioners responded that they used predictive coding for discovery productions, early case assessment and pre-litigation investigation among other things. Companies are demonstrating a growing acceptance of predictive coding among practitioners – but they are not the only ones.

Courts all over the country are actively encouraging the use of the sophisticated technology in lieu of outdated methods, particularly in big cases. In *New Mexico State Investment Council v. Bland*[1], the federal district judge cited one party's claims that predictive coding "[e]nabled the reviewers on the document analysis teams to work more efficiently with the documents and identify potentially relevant information with greater accuracy than standard linear review."

Meanwhile, a New York federal district judge held in *Federal Housing Finance Agency v. HSBC*[2], that predictive coding had a "better track record in the production of responsive documents than the human review."

The Buzz Around Social Media

Another hot topic was social media. More legal professionals are dealing with social media in connection with their ediscovery obligations today as compared to 2013. Companies have begun leveraging platforms like Facebook, Twitter and Snapchat to build relationships with their targets and market their products. The use of social media provokes a plethora of ediscovery questions, including privacy, discoverability, preservation, collection and authentication issues. Nonetheless, more than 50% of respondents to Kroll Ontrack's 2014 ediscovery trends survey were involved in matters that used social media data.

Similarly, the federal courts have been dealing with social media and other types of "unique" electronically stored information – in particular, courts have begun to ask whether social media, texts, voice memos, and even personal computer data should be preserved in anticipation of litigation. Generally, the preservation question hinges on whether the information is relevant to the case. In *Calderon v. Corporacion Puertorriquena de Salud*[3], the court ordered sanctions for the failure to preserve text messages, and the court in *Painter v. Atwood*[4], ordered preservation of both text messages and Facebook messages. This trend is tangential to another issue – whether the "bring your own devices" (BYODs) that so many employees carry with them are now discoverable. Currently, 58% of companies have dealt with ediscovery matters involving BYOD preservation questions, according to Kroll Ontrack's ediscovery trends survey.

The Importance of Cyber-secuirity

While the duty to preserve is still analysed on a case-by-case basis, another duty – that of cybersecurity – is paramount in the United States. With major data breaches at prominent retailers, companies in the US have discovered they have a duty to secure both their own data and that of their customers. Over 62% of law firms and corporations in Kroll Ontrack's survey indicated that security concerns impact their ediscovery practices, and they consulted either internally or externally regarding those concerns. Further, while corporations are learning to work with specialists to protect their data, law firms realise they are a "back door" to critical corporate information. Under the American Bar Association Model Rule 1.6, lawyers have a duty to prevent the inadvertent or unauthorised disclosure of or access to client information. For this reason, cybersecurity is an ethical imperative for American lawyers, and better visibility into cybersecurity practices associated with ediscovery is a necessary area of development in 2015 and beyond.

Looking Forwards

Overall, 2014 was a lively year in American ediscovery: the courts have embraced predictive coding, the explosion of social media and BYOD has raised questions about the duty to preserve, and corporations and law firms are increasingly concerned about cybersecurity. As we move forwards, these topics will remain relevant – but so will the emerging issues surrounding information governance, the Federal Rules of Civil Procedure amendments, and the improved use of analytics to search big data.

by Jonathan Sachs
Strategic Markets Director, Kroll Ontrack
jsachs@krollontrack.com

1 2014 WL 772860 (N.M. Dist.)
2 2014 WL 584300, (S.D.N.Y. Feb. 14, 2014)
3 992 F. Supp. 2d 48, 50 (D.P.R. 2014)
4 2014 WL 3611636 (D. Nev. July 21, 2014)

EDISCOVERY IN ASIA

AN INSIGHT INTO BEST PRACTICES

This article was first published in ILTA's May 2015 issue of Peer to Peer titled: "Litigation and Practice Support" and is reprinted here with permission.

Ediscovery in the APAC region is a young industry with numerous opportunities for growth. As international business transactions and global litigation become more prevalent – and Asian economies flourish – practitioners must be aware of how to handle ediscovery in APAC by understanding the culture, differences in the way in which technology is used and business practices. Further, practitioners must be aware of the constant change in the legal landscape and potential conflicts between countries and regions and legal systems. Overall, APAC ediscovery law has proven to be extremely fluid; thus, it is important for practitioners to keep afloat in these ever-changing waters

Most of the countries in the APAC region have civil law jurisdictions, as opposed to common law legal frameworks similar to those in the US or UK. Hong Kong, Singapore and Australia do, however, have a common law system. Given this variation and with ediscovery in APAC still in the early stages of development, it is hard to make sweeping and general statements that apply across the entire region. The best approach is to consider each country's laws and customs individually, but some general themes do apply:

The Legal Climate: Discovery v Privacy

Some APAC countries such as Hong Kong and Singapore have created special rules for the discovery of electronic data. However, data privacy and confidentiality pose the biggest challenges for APAC ediscovery projects. Many ediscovery professionals have expressed concern about new laws forming in the APAC region around the topic of data privacy. For example, Hong Kong, Singapore and Japan have adopted (or are in the process of adopting) data privacy regulations. Hong Kong uses traditional English discovery law, which makes Hong Kong the APAC country most amenable to American-style ediscovery procedures. Singapore is also open to discovery and is equally as advanced, given its recent adoption of aggressive measures to become the premiere dispute resolution hub in the region. Japan has likewise begun deliberations on the implementation of ediscovery laws, but the Japan Privacy Act makes conditional and limits the transfer of personal information from a corporate entity to a third party.

New regulations regarding electronic data are anticipated in Japan, Hong Kong, Singapore, China, South Korea and Taiwan. Given the differences in privacy expectations between the US and APAC regions, these potential changes will impact on the ediscovery landscape and will need to be monitored.

Cost Control

Similar to the situation in other parts of the world, another concern with ediscovery in APAC is the associated cost. Many APAC companies are uncertain of how much they spend on discovery and are unfamiliar with the cost dynamics of ediscovery as the costs are often incurred in US litigation. Additionally, as many APAC companies come from a different litigation system and culture and have difficulty understanding the purpose behind the production of data, they have difficulty accepting the costs and feel that discovery creates an unnecessary burden. Because of this, it is important for lawyers to be up front with APAC companies and thoroughly explain the costs involved in litigation. Furthermore, it is important to explain the purpose behind discovery requests and the role that discovery plays in uncovering and narrowing the key issues in dispute in a case and paving the way to a settlement that reduces the overall legal costs associated with litigation.

Multi-Country Matters

In the APAC region, it is not uncommon for a single legal matter to have data collection and preservation efforts across multiple national borders. Further complicating matters is a regional and global trend toward cooperation among regulators from different countries, which in turn is creating more multi-country cases requiring ediscovery.

In addition to these overarching issues, the following distinct legal paradigms subsist in the APAC region:

JAPAN

The Personal Information and Protection Act of 2003 restricts the collection, use and transfer of personal data. In addition, as already mentioned, the Japan Privacy Act limits the transfer of data from a corporate entity to a third party. These kinds of privacy restrictions add to the complexity of ediscovery. Currently, Japan has no law that directly addresses ediscovery.

SOUTH KOREA

Perhaps the most challenging ediscovery environments are those of South Korea and China. While ediscovery law in South Korea is still relatively undeveloped, several laws protect the processing of personal information. Additionally, the 2011 Act on the Protection of Personal Data requires many businesses and government agencies to provide data breach protection.

CHINA

China deals with data protection and privacy issues on a piecemeal basis, and a central framework for governing ediscovery matters has yet to be established. Moreover, China's ban on the transfer of "state secrets" (a term that carries a vague and broad definition) creates a significant barrier to compelling production of information in international litigation. Data from China is, however, frequently targeted in US litigation and international investigations. In addition, China does not formally allow or require the discovery of information relevant to litigation. China's regulations often are in direct conflict with international rules, regulations and judicial orders. All documents must be reviewed and cleared of any secrecy concerns before they are allowed to leave China which makes it critical to process data for ediscovery locally. However, many courts and regulators outside of China are unsympathetic to this issue. We recently conducted a market study on ediscovery in China. To read more about the cases it is being used on and how it is being carried out see our website at www.ediscovery.com/cms/pdf/Ediscovery-in-China.pdf.

HONG KONG

Hong Kong follows a common law structure and discovery process similar to the US. Order 24 of the Hong Kong Rules of High Court provides a discovery framework that allows courts to limit discovery to forward objectives like "cost-effectiveness," "fairness" and "expeditious" dispute resolution. More recently, however, the Hong Kong judiciary has considered plans to issue a comprehensive practice direction to address ediscovery head-on, based on on the practice direction that is in use in the UK (Practice Direction 31 B on the Disclosure of Electronic Documents).

SINGAPORE

As a common law country, Singapore used to have an "opt-in" approach to ediscovery, but in 2012 it amended its discovery regime (Practice Direction 3 of 2009) to allow courts to order ediscovery without the consent of the parties. The new rule emphasizes the importance of proportionality, search and key word testing.

APAC Ediscovery: 8 Tips and Tactics

APAC ediscovery arises in various different types of cases. While the majority of cases stem from US or EU litigation, a large portion of APAC ediscovery results from cases that involve regulatory requests, internal investigations (most often relating to the Foreign Corrupt Practices Act in the US or the UK Bribery Act), and company-driven internal compliance reviews.

Handling these APAC ediscovery issues may seem like a daunting task but the following practical tips help navigate the differences in culture, technology and business practices:

1. Understand the Need to Straddle More Than the Language Divide

Most APAC companies cannot fathom why an American court would require a party to collect and exchange massive amounts of data. Lawyers that need to collect and process data from APAC should be prepared for this disconnect and know how to handle communications. This goes beyond proficiency in an Asian language and goes into educating clients about the international discovery process.

2. Start Preservation Early

Most APAC companies are unfamiliar with document retention obligations that attach in the international once a lawsuit is filed. Moreover, many of these companies may not even have electronic document storage and recovery systems in place. Parties that need to collect data in APAC are well-advised to quickly preserve data even if the course of action for litigation is not yet clear.

3. Be Cautious of Nationalist Challenges

Strong nationalism may thwart data collection efforts, as parties question why APAC privacy considerations do not trump foreign discovery laws. Tread lightly with this matter to avoid further bumps in the dispute resolution process and make sure that you thoroughly explain the reasoning behind each discovery request.

4. Capture Full Forensic Images and Conduct Client Interviews

Because of geographical and nationalist challenges in APAC, a lawyer cannot risk an inadequate collection. As such, comprehensive collection methods and not just an active data capture is recommended in the APAC region. Along the same lines, it is important to ask custodians for all spelling variations of their name during the client interview.

5. Be prepared for International Data Nuances

In the APAC region, software is often vastly different and multilingual software platforms generate different metadata fields. Finally, use of free email packages is more prevalent, and a lawyer may need to collect electronically stored information from several email systems.

6. Don't expect data to be easily accessed

APAC companies frequently encrypt their data, creating obstacles for ediscovery professionals. It is advisable to build a workflow into collection, processing, and review for handling any password protected or encrypted documents. Additionally, keep a list of passwords found during document review, and be prepared to use password cracking software.

7. Don't Overlook the Paper

APAC companies still rely heavily on paper documentation. Ediscovery professionals need to pay special attention to paper in the APAC region, given that paper sizing and hole-punching may be different. Optical Character Recognition (OCR) is often not available for many languages.

8. Make Friends and Work with Local Counsel that Understand Local Best Practices

Perhaps most importantly, it is well worth building relationships with APAC legal discovery experts. Local counsel experienced in ediscovery collections or local service providers can greatly assist by acting as a mitigating party, explaining sovereignty issues, integrating paper and data into one database, and collecting data before spoliation occurs. Do not be caught evaluating international data transfer, privacy, and security requirements after data has been transported out of a country or region.

Conclusion

Although there are a multitude of differences, several universal best practices hold true across the globe for ediscovery. For example, IT and legal departments must be on the same page, technologies must be validated, and service providers in the region must be thoroughly vetted.

APAC is clearly experiencing a rapid development of privacy rules and ediscovery rules are evolving too. Companies that need to collect data in these countries for discovery purposes will need to address legal restrictions on data access and transfer by focusing on legal approaches and technology solutions (such as local data processing) to iron out difficulties. Similar challenges in Europe are being successfully overcome and best practices can be shared and taken advantage of in APAC.

by Kate Chan
Regional Managing Director, APAC, Kroll Ontrack
kchan@krollontrack.com

The Nordic landscape

The Nordics' thriving energy, technology, and defence businesses are exposed to the risks of international trade as well as competition regulations, making the prospect of investigations commonplace.

Sweden and Norway have both seen their share of large scale investigations with companies investigated for fraud, corruption and other malfeasance in which lawyers and in-house counsel have needed to apply the latest technology in order to review and assess vast quantities of unstructured data.

Whilst none of the Nordic countries have a formal ediscovery regime in place, there is increased use of electronic evidence tools in corruption cases, internal investigations, and dispute resolution. This is largely for the following reasons:

- There is now so much data that even the smallest investigations need electronic evidence tools to make the exercise efficient.
- Younger lawyers in the Nordics have been exposed to ediscovery practices whilst working at US or UK law firms and advocate the benefits that such technologies can offer.
- The myth that ediscovery services are so expensive that they could only be used in the largest cases has been broken. Ediscovery is routinely considered for smaller investigations.
- Industries in the region are particularly keen to protect their intellectual property and electronic evidence services are especially useful for investigating industrial espionage and IP theft.
- National Courts, at least in Norway, appear to welcome the use of electronic evidence tools in certain cases.

Risks in the Nordics

Transparency International (a non-governmental organization that monitors and publicises corporate and political corruption in international development) ranks each of the Nordic countries within the top 5 *least* corrupt countries in the World, which is a great achievement.

The biggest industries in Nordic countries such as energy and oil companies are exposed to risks related to international embargoes and sanctions and corruption. As many companies are subject to the rules relating to the Foreign Corrupt Practices Act (FCPA) and the Bribery Act, infringement could be criminal and the consequences may be severe penalties, including prison sentences and of course, damage to the reputations of individuals and the companies concerned.

There is a low tolerance in the Nordics for the failure to apply business standards. Reputational damage can lead to exclusion from public tenders and there have been several high-profile cases that illustrate this point. Last year, one public-sector case involving the Norwegian bus company Unibus resulted in one person sentenced to a total of 23 years and 9 months in prison for their part in a case in which vehicles were bought from Germany illegally. The Nordic countries take corruption very seriously.

Cost Effective Investigations

The same as in other European economies, the cost of running an investigation is likely to be controversial. In Norway, shareholders can propose a corporate investigation with a specified subject and if that motion is carried, the company itself (rather than its shareholders) must pay the costs of the investigation. Meanwhile, a Norwegian Court, considering the well-publicised Troms Kraft investigation, refused to grant the recovery of a significant portion of the costs to the investigator company charged with the investigation. This puts high demand on efficiency in conducting investigations in the region.

Within this context, electronic evidence tools will assist to reduce the number of hours spent reviewing data from electronic sources of evidence, which in turn reduces the amount of cost associated with carrying out such investigations. It is likely that firms looking to carry out internal investigations will be looking to bring more certainty to the forecasting of costs and that may drive an increase in fixed fee arrangements.

Who is Using Electronic Evidence Technology?

PRIVATE COMPANIES

Second to law firms, the primary users of ediscovery technology and services in the Nordics are private companies. Many national and international companies have their own investigations teams situated in-house, for the purpose of investigating industrial espionage and intellectual property theft. National courts are increasingly ordering the collection of evidence to help establish the facts behind suspected team moves, a problem which particularly impacts the technology industry.

THE COURTS

In some cases the courts have appointed computer forensics experts to support the bailiff in the seizure of any information assets from houses, cars, and offices. Information contained on such assets (which may include laptops, hard drives and telephones) would be preserved and then filtered using search terms agreed between the parties, prior to making the evidence available for review. This, in a country which has no formal ediscovery rules, is the closest that we have seen to an emulation of the discovery rules which are regularly exercised in the US and in the UK. Once the documents have been filtered they are presented in a database which the judge uses to review the documents to identify and to remove privileged material.

The Future

Looking ahead it is expected that many more of the law firms practising in the region will realise the benefits of having assistance in securing and collecting electronic evidence.

It is true that many legal practitioners do not currently realise the complexity of running an investigation using electronic evidence until they are in the midst of one. This is a turning point for those with experience, as this is the time that they realise the need for ediscovery guidance and expertise in planning cases before taking them to Court.

As knowledge among Nordic practitioners increases and best practices are shared, it is anticipated that more firms and companies will crave the strategic advantage of being prepared.

by James Farnell
Legal Consultant, Kroll Ontrack
jfarnell@krollontrack.com

The growing demand for ediscovery in Switzerland

Despite its small population of just 8 million people, Switzerland is one of the world's most powerful economies, boasting a GDP of $685.4 billion.[1]

Because of the favourable environment, Switzerland is a centre for international business, with many of the world's largest corporations and financial institutions calling Switzerland home or having a base there.

Yet even though Swiss law contains no requirement for ediscovery, there is a growing demand and need for ediscovery technologies in Switzerland.

Private Banking and Intense Regulatory Scrutiny

Switzerland is the home of many private banks and up until recently they were protected from foreign investigation by Switzerland's famously stringent bank secrecy laws which forbade banks from revealing any information about account holders to third parties, including tax authorities, foreign governments or even Swiss authorities, except when requested by a Swiss judge's subpoena.[2] However in 2013, the Swiss government signed up to an international convention that sets out the framework for countries to assist each other with requests for tax information.[3]

These changes led to a cascade of regulatory initiatives focused on banks, particularly private banks thought to be working with foreign nationals who were using the banks as a means of evading tax.

Two initiatives have had a particular impact on Swiss banks. The first was the US Department of Justice's "Swiss Bank Program", introduced in August 2013. Swiss banks were given until December 31st 2013 to enter the programme and advise the DOJ that they had committed tax-related criminal offenses in connection with such undeclared US-related accounts. In return, banks joining the scheme are eligible for a non-prosecution agreement if they meet all the requirements, including full disclosure of cross-border activities.

Secondly, for those not complying, there is a risk of being investigated and heavily fined. In 2014, Credit Suisse was fined a record $2.9 billion. US Deputy Attorney General James Cole said, "Credit Suisse's lack of effective cooperation was an important additional factor in determining the resolution of the case. Put simply, cooperation matters."

What Does Increased Regulatory Scrutiny Mean for Ediscovery in Switzerland?

Increased regulatory scrutiny has and will continue to result in both increases in compliance efforts and in ediscovery in litigation.

What Concerns and Preferences Do Swiss Ediscovery Clients Have?

Security of data is of prime concern for Swiss companies undergoing investigations and a great deal of emphasis is placed upon the need for providers of ediscovery services to operate from within Switzerland. Swiss ediscovery clients also strongly prefer ediscovery providers to process data locally.

Our research also indicates that confidence in a vendor's ability to protect privileged information is a key deciding factor in choosing an ediscovery partner.

Ediscovery Challenges that Arise in Switzerland

Swiss data protection law does not necessarily allow an employer to access the emails of employees even if stored on company servers. Companies therefore have to ensure that they do not access the personal emails of employees when assembling data for the purposes of discovery in legal cases. Data protection rules also apply to business emails to, from and about clients and other third parties. The processing of large volumes of business emails as part of US or UK discovery procedures may be considered to be excessive processing of personal data which is not permissible. To add to the complexity, Swiss information cannot be made available overseas without ensuring an adequate level of protection for this data is in place.

Two other obstacles arise in relation to the discovery of Swiss data as set out in Article 271 and 273 of the Swiss Penal Code, the first of which prohibits the taking of evidence in Switzerland for use in a foreign legal proceeding without judicial assistance and the second of which prohibits disclosing the business secrets of third parties in Switzerland without permission.

Against this complex legal backdrop, computer forensic specialists are often hired to help search for the relevant documents needed in cases to ensure a targeted collection takes place to comply with data protection law. The data is then filtered to try and identify potentially relevant private emails. Swiss lawyers who are privacy experts are often hired to redact business emails containing personal content before they are produced in proceedings.

Cross border data transfers from Switzerland to other countries need to be done on a very restricted basis. There are various mechanisms for handling this challenge including filtering the data in country before transferring it and the use of data transfer agreements which allow documents to be reviewed outside of Switzerland.

At Kroll Ontrack we have responded to requests made by our clients and developed a mobile discovery solution for use in-country or at client premises in Switzerland to avoid unlawful data transfers out of Switzerland, to data centres in Europe and the US and to give our clients control over their data.

What the Future Holds

On March 30 2015, the DOJ announced that it had entered into a non-prosecution agreement with BSI SA under its Swiss Bank Program, with the bank agreeing to pay a fine of $211 million.[4] Compared to other Swiss banks such as UBS and Credit Suisse who have received proportionally much larger fines, this resolution will perhaps see many more Swiss banks joining the Swiss Banks Program and other similar initiatives.

As more banks and other financial institutions face regulatory investigations or join schemes such as the Swiss Bank Program, ediscovery solutions will become a high priority for banks in Switzerland.

by Tracey Stretton
Legal Consultant, Kroll Ontrack,
tstretton@krollontrack.com

1 http://data.worldbank.org/country/switzerland
2 http://www.kpmg.com/CH/de/Library/Legislative-Texts/Documents/pub_20090101-BankA.pdf
3 http://www.ft.com/cms/s/0/05c2d098-9bed-11e4-b6cc-00144feabdc0.html#axzz3ZNKenPBt
4 http://www.lexology.com/library/detail.aspx?g=e1c8a33c-761f-4b0b-a733-d80f37fe23be

Getting a taste of disclosure in Belgium

As a civil law jurisdiction, there is no formal requirement in Belgium to exchange evidence prior to and in the course of litigation.

The activity of identifying, reviewing and producing evidence required for disclosure between parties that has propelled much of the growth of the ediscovery industry in the US and UK is therefore almost non-existent in Belgium.

Dispute Resolution in Belgium

This is not to say that law firms operating in Belgium are immune from the issues created by the increases in volumes of electronic data held by their clients. Young lawyers (in particular) from national firms are increasingly keen to find new efficiencies using electronic evidence tools in order to locate, manage, and investigate evidence in their cases. Whilst using document review platforms is still not the norm for many lawyers in Belgium, there is an eagerness to understand the technology that is available, and a need occasionally to rely on specialist forensic services to, for example, recover deleted data, or uncover data theft when this is required for a case.

EU Activity

As the major decision-making centre in the European Union, Brussels is the 'de facto' capital of Europe due to the number of European and International Institutions located in the city. The vast majority of ediscovery activity in Belgium is concentrated on assisting law firms and corporations that need to respond to investigations led by the European Commission's Competition Directorate General, DG COMP. Such investigations may concern suspected cartel behaviour, abuse of dominance issues or the potential effects of proposed mergers. It is not a coincidence that each of the major international law firms has an office in Brussels in order to keep an ear close to the ground with respect to on-going activity at the Commission.

Dawn Raids, Technology and Fines

Recent enforcement activity by DG Comp has been significant. Total fines imposed this year by the Commission for anti-competitive activity was 1,670,012,000 Euro. DG Comp Head of Unit in the Cartels Directorate, Mr Dirk Van Erps, has made a point of adopting state of the art technologies to search and manage electronic evidence during competition investigation Dawn Raids. This has increased the pressure on companies and their legal teams to ensure that they are likewise also equipped with the latest technology to rapidly detect any infringement (hopefully) before the Commission does, or another cartel member pleading for leniency.

The reasons for businesses to take preventative action in the face of the Commission's enforcement regime have been made abundantly clear. The fines levied on corporations found to have infringed EU Competition rules can be up to 10% of global turnover. This does not include the additional possibility of follow-on litigation (the new Directive regarding Civil Damages actions for Antitrust infringements now having been adopted), an additional measure spearheaded by the Commission in order to further increase pressure on companies to clamp down on cartelist behaviour.

In the face of such enforcement, or threats to the success of a proposed deal, many companies take pro-active steps to investigate their own employees in order to locate, isolate and deal with such infringements, to prevent them occurring in future. In addition to such steps, re-considering company policies relating to the storage of data, appropriate training of IT teams (should a dawn raid occur under their watch) as well as understanding where company data is located are paramount. These are among the important new technological challenges business leaders and in-house counsel need to face up to in order to mitigate the risk of a cartels unit that is willing and ready to literally 'plug in' to their IT infrastructure.

More Enforcement to Come

The vigour with which the Commission enforces Antitrust rules within the EU is not set to wane over the next five years. Jean-Claude Juncker who will be presiding over the Commission for his next term has a packed agenda to increase jobs, growth, investment and competitiveness within the EU, and has specifically singled out the digital market as requiring reform.

Key Sectors to Watch Out For

It is widely expected that Juncker's European Commission will target the Energy, Digital, Financial and Telecoms markets. Competition continues to play a very central role throughout the EU, especially given current economic uncertainties and the Commission's stated aims.

What is also clear is that intense enforcement will implicate non-EU companies in the same way as EU companies. Margarethe Vestager (the new Competition Commissioner) plans to engage in cooperation with other jurisdictions (including the emerging economies).

What is the Ediscovery Future for Belgium?

Looking ahead we can expect to see ediscovery trends such as the following:

- Renewed competition enforcement activity in the Digital , Energy, and Financial sectors
- Internal investigations and proactive data management measures to be carried out by companies who feel most at risk
- Co-operation between international agencies will foster new best practices. The European Commission may follow in the steps of the DOJ by developing a model protocol for the use of Predictive Coding technology in Competition cases
- Uses of technology for litigation and arbitration matters in Belgium will increase gradually.

by James Farnell
Legal Consultant, Kroll Ontrack
jfarnell@krollontrack.com

New Frontiers in Italy & Spain

The data explosion and developments in regulatory powers have caused a change in the way that lawyers in Italy and Spain, as well as other parts of southern Europe are handling document review projects.

Attitude Towards Ediscovery Technology

The adoption of ediscovery technology for the systematic review of documents has been slower than in other parts of Europe, largely due to the lack of a discovery regime in litigation, but also due to a plentiful supply of low-cost (or free) interns resulting from economic troubles brought by the last recession. The result has been little exposure to the benefits of managing data in hosted ediscovery systems, therefore it is unsurprising that there has not been a widespread plate-shift towards the use of ediscovery databases in investigations, even in the face of growing data sets.

Instead, ediscovery has in the past been seen as a process that adds cost and its application in legal matters was deemed to be a luxury for use on only those matters with the highest stakes at risk. This was reflected to some extent by the character of the companies and their law firms who tended to use such technology. Large international players with corporate headquarters outside of Italy and Spain would drive ediscovery efforts in cases that often have more complex cross-border issues.

The Time for Change

In 2015, the situation is set to be noticeably different. One reason is that the Italian Competition Authority (*Autorità Garante della Concorrenza e del Mercato*) and the Spanish Competition Authority (now integrated in the *Comisión Nacional de los Mercados y la Competencia*) are both more active in investigating cartels. In such matters, speed and efficiency in the race for leniency is essential. As data volumes are generally increasing there is a craving for efficiency and to find information faster and the sole reliance on tools used for an indepth forensic analysis is no longer appropriate in many cases. The scene is set for companies to rely more on document review tools.

The Spanish Competition Authority has itself recently introduced an automated electronic evidence submission procedure (sede electrónica) allowing *inter alia* merging parties to electronically submit merger notifications and pay administrative procedural fees online.

Another reason is that the level of competition between law firms is increasing. Ediscovery technology is being leveraged by those firms that seek to differentiate themselves on capabilities rather than costs. More firms are offering to do internal investigation work on a fixed fee basis, which heightens the need to work quickly and on point. At the same time, boutique firms with expertise grown inside large international firms are presenting formidable practices with ediscovery expertise as a valuable add-on. Having the know-how and agility to navigate complex data issues is emerging as a clear business advantage.

At this time, the charge towards ediscovery technology is being led by lawyers in private practice who can clearly articulate the advantages to their clients. Companies that are not regularly exposed to disputes or regulatory intervention are in need of education about the potential issues that they might face at some ill-defined 'point in the future', which is hard to forecast. For this reason it is an uphill struggle to get board approval to invest in developing a formal approach to ediscovery.

Starting with Compliance Audits

What is perhaps easier to monitor are activities and developments among competitors, suppliers and customers, which can be spelled out in terms of opportunities and risks. In one sense this can be aimed at anticipating issues such as regulatory non-compliance and corruption, which could lead to significant fines and costs to the company. By deploying ediscovery technology in small scale compliance audits (exercises in which typically 6 to 12 months of emails for a number of higher-risk individuals are reviewed in search of evidence of any potential issues), a steady rise of companies in Italy and Spain are putting themselves in the position where they can decide whether to blow the whistle on any illicit practices that they might discover. At the same time those companies that have have established compliance programmes will be shown extra leniency if later found by the Italian Competition Authority to have infringed national competition law. This concept was introduced as a formal incentive to increase compliance in 2014. Companies that are developing compliance programmes often find that the benefits continue when they expand such programmes to include spot-checks on the company's own preparedness to react to a surprise investigation. A thorough compliance programme should also consider checks on electronically stored evidence as this often results in problematic behaviour being uncovered early enough for it to be dealt with.

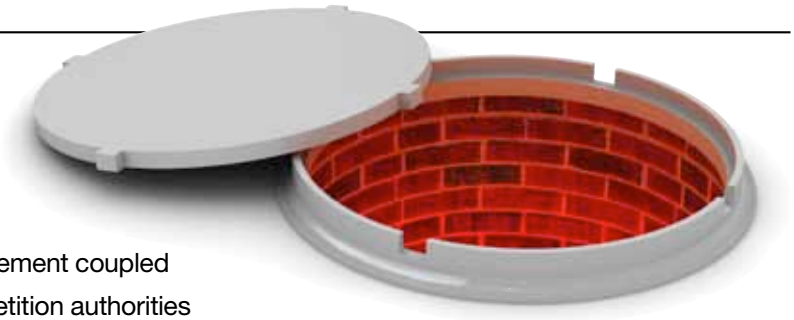
Ediscovery practice is also becoming more of a feature in pre-merger due diligence and regulatory clearance. In such cases, the goal is to get the deal through, so it is generally more accepted that a team focused on such an important objective must have the proper tools to conclude their business effectively, in full compliance with the regulator's requests.

New enthusiasm for Legal Technology

In summary, there has been a birth of new enthusiasm for technology in Italy and Spain, which has been brought about by the evolution of regulatory laws and practices but also an inevitable yield to big data volumes. There is an upward curve in the number of internal compliance investigations but this is likely to have a relatively low trajectory as businesses continue to learn about the advantages of technology in investigations and lawyers continue to equip themselves with relevant skills and knowledge.

by Tina Shah
Legal Consultant, Kroll Ontrack
tshah@krollontrack.com

UNCOVERING CARTELS



The year 2014 was among the most active for cartel enforcement coupled with the increased powers of European and national competition authorities and international cooperation between them on investigations.[1]

The introduction of a wide array of regulatory developments including the recently approved European Directive on Antitrust Damages Actions,[2] the enactment of national laws on collective redress in cartel damages actions such as in France[3] and a major overhaul of EU's Data Protection Rules[4] also stress the increased importance of data and electronic evidence and its crucial role in litigation.

In this vein, the new Competition Commissioner Ms. Vestager recently mentioned that "…data is the new currency of the internet" and that companies managing "big data" should not escape the application of competition rules.[5]

Responding Proactively to Competition Authorities

Over the last five years cartel fines imposed by the European Commission have surpassed 8 billion euros which represents an increase of 161% compared to the level of fines imposed during the period 2000-2004. In 2014, the highest fine imposed by the Directorate General for Competition ("DG Comp") in a cartel case on a single undertaking was over €370 million.[6]

The increased level of fines, investigative powers and enforcement – often through sector enquiries and dawn raids – of competition authorities across the globe force companies to be more proactive in order to detect potential anti-competitive behaviour in their organisations.

Companies increasingly use ediscovery providers to carry out internal investigations as soon as the DG Comp or a national competition authority has carried out a sector enquiry – sometimes in an upstream or downstream market – in a sector where the company in question directly or indirectly operates. In other cases companies have a suspicion that anti-competitive behaviour might be taking place in one of their subsidiaries. These internal investigations would typically include the collection, review and analysis of data (mostly emails and file attachments) from company devices or even personal devices used for corporate purposes following the "bring your own device" policies that an ever increasing number of companies implement.

Since competition authorities all over the world including the European Competition Network now require companies to have IT readiness and antitrust compliance programmes in place, an increasing number of companies are keen to carry out so called "mock dawn raids".[7] These simulated dawn raids are typically carried out by law firms assisted by ediscovery providers to test the IT readiness and compliance measures in place in a company.

Anti-Trust Training

Although aggressive approaches to "mock dawn raids" are possible whereby the ediscovery provider and accompanying lawyers would seek to emulate the *modus operandi* of the DG Comp officials, these are unpopular and infrequent. Companies prefer a cooperative approach so that employees are for example given an antitrust refresher course by lawyers while data from company devices would be collected in the framework of a compliance exercise. When the purpose of such an exercise is openly revealed to employees they are more likely to cooperate and the objective of instilling a compliance culture amongst all employees at all levels is usually more effective.

Uncovering Cartels

Most cartels are uncovered thanks to so called "whistle-blowers" through leniency programmes but once these are revealed it is a race against the clock, or a "race to leniency", to rapidly identify incriminating evidence to obtain a "marker" for full immunity or a reduction in the potential fine, most of which is electronically stored information ("ESI").[8]

This is where technology comes into play, especially in time-sensitive cases, because ESI very often "hides" information – for example metadata that could be crucial in a case or simply hidden columns that conceal pricing information in an Excel table – that can be easily revealed by anyone using ediscovery review platforms.

In certain cases, the functioning of cartels is much more complex. For example, members of the freight cartel that was revealed to the DG Comp in 2012 used code terminology such as "marrows" and "baby courgettes," to surreptitiously refer to surcharges on certain trade routes.[9]

In July 2014, the German *Bundeskartellamt* also imposed over €338 million in fines in a major price fixing cartel concerning sausage manufacturers that was revealed thanks to an anonymous tip-off.[10] Given that this cartel had been operating for decades undetected it is a true reflection of the complexity of cartels and of the use of concealed means of communication by cartelists.

The Role of Technology

As a consequence, many companies rely on advanced tools that allow them to fully visualise and rapidly identify relevant information such as analytics and intelligent review technology (IRT), including predictive coding technology. This is especially relevant since the use of predictive coding technology has recently been approved by an Irish Court (High Court of Ireland) saying "The evidence establishes, that in discovery of large datasets, technology assisted review using predictive coding is at least as accurate as, and, probably more accurate than, the manual or linear method in identifying relevant documents".[11]

In summary, in light of the increased fines and regulatory developments, companies across the globe are becoming more proactive by carrying out internal compliance investigations and "mock dawn raids". In that respect, the use of technology and support from international ediscovery providers who can help companies to emulate the experience of a co-ordinated raid is crucial.

by Thomas Cavro Du Pont
Discovery Services Consultant, Kroll Ontrack
tcavrodupont@krollontrack.com

1 Please see ECN Recommendations entitled "Investigative Powers, Enforcement Measures and Sanctions in the context of Inspections and Requests for Information" and "on the Power to Collect Digital Evidence, including by Forensic Means" dated December 2013

2 Directive of the European Parliament and of the Council on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union

3 "Loi Hamon" n° 2014-344 of the 17th of March 2014

4 This overhaul has been conducted through a proposed Regulation and Directive

5 Hearing before the European Parliament of Competition Commissioner Margrethe Vestager on 2 October 2014

6 Most recent cartel statistics from DG COMP can be obtained online at http://ec.europa.eu/competition/cartels/statistics/statistics.pdf (last updated on 5 September 2015). In 2014, the highest fine in a cartel case was imposed on the German undertaking Schaeffler in the automotive bearings cartel case

7 Please see ECN Recommendation "on the Power to Collect Digital Evidence, including by Forensic Means" dated December 2013

8 The European Commission's leniency programme was first introduced in 1996 and revisited in 2002 and 2006. Many countries all over the world and especially in Europe have also introduced leniency programmes at a national level emulating the European's Commission programme or even by going beyond and improving it

9 Please see European Commission press release dated 28 March 2012 http://europa.eu/rapid/press-release_IP-12-314_en.htm

10 Please see press release from the German Bundeskartellamt available at http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2014/15_07_2014_Wurst.html

11 Irish Bank Resolution Corporation Ltd & ors -v- Quinn & ors [2015] IEHC 175

Global financial services

Since the beginning of the financial crisis regulatory authorities have levelled more than £160 billion in fines to the global banking and financial services industry.

With increased inter-agency cooperation becoming the rule instead of the exception, the levying of fines and penalties shows no signs of letting up. In fact, regulatory agencies charged with investigating fraud and marketplace transactions are reporting that more than 60% of new matters involve cooperation between multiple foreign agencies. This atmosphere coupled with increasing calls for transparency and regulation require paradigm shifts in big data management and legal strategy.

While these shifts occur, the ongoing review of billions of pages of electronically stored information, millions of hours of audio and chat room conversations continues on a daily basis. Financial Services regulations deliver some unique challenges to companies seeking to minimise present costs and future risks. Lessons continue to be learned on how to manage and mitigate investigations and litigation arising from the current situation. A few of them are gathered here.

Information Governance

On occasion, it has become clear that some financial services organisations did not expect the scale of requests for information or the volumes of data that would one day need to be retrieved. "Save everything" policies that crudely secure the data, offering initial cost savings will cause major headaches as information requests roll in. How data is catalogued for retrieval, how it is archived, where it is archived and ease of access are considerations that many companies in every sector are unfortunately looking at in hindsight because in practice it can take a lot longer than expected to gather all of the information that is needed with any certainty. Even if data has not been stored for optimal retrieval at short notice, it is possible to retrospectively organise it in one place, so that cursory searches for emails and documents belonging to custodians or groups can be performed quickly and accurately in the identification stage of the Electronic Discovery Reference Model (EDRM). However, this type of exercise can be costly and such reform begins with consistent data retention and a records management policy (that imagines the scenario of time-pressured retrieval of specific data) driven by the legal department across all business units.

Collection

Many banking and financial services companies with multi-national locations underestimate the time required to perform a comprehensive collection of data. For some organisations this is more complicated than they imagine because of the sheer reach of their data estate (many organisations have expanded globally through mergers and acquisitions or buyouts and have not necessarily incorporated all IT systems into one). The time it can take to find, restore, copy, and ship that data can be considerably lengthy. In one instance, the restoration of email from back-up took three months; two months later than required by the regulator. In another, the internal resources needed to extract the relevant audio files were deployed on other matters. To add insult to injury, the legal department had to wait for the hard drives to be shipped after being delayed by customs at the border, meaning that a request for an extension to the Financial Conduct Authority (FCA) became necessary. Proof, perhaps, that every moment in planning saves three or four in execution, such complications are not always foreseen and the contingency advice that can be offered by an experienced ediscovery consultant becomes extremely valuable.

Review

The specialised tools used during the day to day operations of the finance industry present many review challenges. Chat rooms specifically designed to stay open perpetually or audio lines recording 24 hours a day make it difficult to delineate the beginning and end of a conversation or a subject. The industry is combatting this with large contractor review teams and electronic review tools with technology that enables predictive searching of documents and searching for relevant sounds in months of audio recordings. Structured data analysis also quickens the pace considerably, by combining human intelligence with technological brawn to expose the anomalies that the keenest human eyes will miss. The technology employed early on can mean the difference between meeting deadlines on budget and missed deadlines over budget.

Production

Internationally there are more than 200 financial regulatory agencies and authorities and while they may cooperate in terms of evidence the requirements for the production of that evidence varies dramatically. The Department of Justice in the United States, for example has specific requirements on all data formats, while other agencies may be less prescriptive about what they receive as long as they are happy with the quality of evidence served. It is sure that with gargantuan data volumes to sift through, everyone welcomes a practical, responsible, ethical and defensible proposal on how to reach the end result as quickly and cleanly as possible. Early planning and negotiation and a clear commentary on how the evidence was found will help avoid possible penalties and sanctions. Being armed with an expert who can explain what the technology can find and what steps to take to mitigate against possibly missing crucial evidence has never been more important.

by Ben Fielding
Account Director, Kroll Ontrack
bfielding@krollontrack.com

Computer Forensics

One of the first and biggest challenges in any search for electronic evidence is creating a logical and technical strategy in order to capture all of the relevant material.

For many years legal teams have used the special skills of computer forensics practitioners to enhance their cases, but have also relied on alternative resources (principally in-house IT experts) in order to manage costs when there is no specific need for a qualified third party expert. The deployment of computer forensics expertise in ediscovery shows that a digital evidence specialist is needed not only to defend your approach to an e-search but could be a vital weapon for more aggressive tactics to win your case.

The Role of Computer Forensics in Ediscovery

Computer Forensics (Digital Evidence Forensics) plays an increasing role in the identification, collection and evaluation of the veracity of data in legal cases. Electronic evidence exists in many forms, on many devices. Identifying the physical location of the data and how it should be collected in a defensible (and repeatable) manner is critical. Often the scoping of an ediscovery project begins with a data mapping exercise carried out with the assistance of a Computer Forensics expert. The preservation of key evidence is a process that is also increasingly guided by forensic experts.

As a science, Computer Forensics has more to do with the metadata surrounding documents (the how, when and where it was created), rather than the content itself and it is the preservation of that metadata which is fundamental, especially in cases where the veracity of evidence is challenged.

There has been an increase in the past year in the use of cloud based storage and applications which increased the challenges associated with performing a collection. Demands from regulatory and law enforcement authorities as well as from businesses seeking general good governance has driven the need for professional help with investigations and collections.

Evidence is often needed at short notice and is often to be found in diverse and disparate sources. Few businesses can truly claim that they know where all of their data is all of the time, making it difficult for most to capture all of the relevant material in a time-bound situation. The increase in cloud based applications and structured data systems (e.g. where a cloud or web based system is used), serves to complicate searches for evidence because the data which the user perceives to exist, as they see it, may actually be derived from many different sources.

Do You Know Where Your Data Is?

In the past, businesses have merely preserved data, accumulating boxes upon boxes of old media, hard drives and tapes for which they have insufficient records of what is contained on the media. In many cases (particularly tapes) the hardware is no longer available and the backup software is also unknown.

There have been a number of cases in the past year where the consequences of not properly documenting data locations and archives have attracted adverse comment.

Because of this, companies undergoing investigations are calling upon computer forensics experts for assistance in collections to ensure data sources have been located and searched. It is becoming increasingly common for computer forensics experts to assist in pro-active audits of data estates so that all data is accounted for and ready for use in any subsequent investigations.

Overcoming the Challenges

Some jurisdictions dictate how data should be collected and preserved. There are principles which are internationally recognised for the collection and preservation of digital evidence. However, increasingly (and rightly so) there is growing legislation surrounding the issues of data privacy and the handling of personal information. Further concerns arise from businesses about transfer of data outside the local jurisdiction. Forensic professionals work around these challenges by filtering data on site so that only strictly relevant information is captured. However, in such cases, the objective, search terms, filtering strategy and tools must be clearly defined at the outset. A mistaken approach or the use of incorrect tools or techniques may result in missing important data. Time spent formulating and agreeing these matters in advance is time well spent.

Forensic Investigations

Computer Forensic investigations are not limited to the largest of cases but are often deployed for smaller less complex cases. Investigations tend to be ordered by HR, IT, Security, Directors, Legal or even the Board within all types of business. The actions of an individual or a cohort are often the concern which prompts an investigation and in some cases of extreme sensitivity, the case must be investigated covertly.

Typical investigations over the past 12 months have been concerned with “inappropriate behaviour in the office”, “IP theft”, “fraud” and “bribery”. Forensic experts have helped to establish timelines, identify key documents, and to determine how communications were sent (identifying pertinent devices, applications and even social media). Cases of alleged hacking and malware have also increased. The forensic securing of media and evidence is at the forefront of these cases.

New Strategies

An interesting turn in the habits of those who instruct computer forensic experts is to use them for aggressive tactics, designed to expose weaknesses in the cases of their opponents. In one instance, a case-turning document, allegedly created five years earlier at or around the time when an agreement was signed, was found to have been created just two weeks before its disclosure. Expert evidence showed that the email was an elaborate forgery, created on a system which mimicked the real system in use at the time.

The Future Landscape

The future seems certain to bring new challenges for companies and Computer Forensics experts. The increase in devices and volumes of data seems inevitable. With this the use of encryption will become a default on mobile devices. The strength of encryption techniques is increasing and so companies will need to ensure they manage encrypted devices to protect their data against unauthorised or accidental access and also so they can access the data on demand when needed and that individuals cannot use their own level of encryption.

By Joanna Ward *Business Development Consultant - Computer Forensics, Kroll Ontrack*
joanna.ward@krollontrack.com

MAN AND THE MACHINE
NEW TECHNOLOGIES IN EDISCOVERY

In the past few years there has been a race towards ediscovery technology innovation, with a suite of advanced tools now available to make the process faster, more accurate and less expensive. Data filtering, Boolean keyword lists, topic grouping/clustering, near-duplicate analysis, and concept searching have all been hailed at various times as revolutionary breakthroughs.

The latest trend in this cycle, Predictive Coding, enables an expert lawyer to teach a computer how documents should be prioritised and categorised.

Predictive Coding

With the advent of 'big data', the traditional linear method of review is becoming increasingly cost-prohibitive for clients.

In fact, the parties in *Irish Bank Resolution Corporation Ltd & ors -v- Quinn & ors*[1] were sufficiently agreed on this point to initially engage in the process of using Technology Assisted Review (or Predictive Coding), at the request of the Plaintiffs.

Predictive Coding aims to combine the legal knowledge of an expert in a given matter, with the repeatability and scalability of advanced technology. A lawyer whose judgment can be safely relied upon, will categorise a sample set of documents. That sample set will then allow the computer to calculate how the remaining documents should be categorised. This can increase both speed and accuracy, whilst reducing costs at the same time. It is important to engage properly in the process and set out a transparent methodology, as these aspects will be critical in convincing other parties and the courts that disclosure responsibilities have been properly discharged, as *Irish Bank Resolution Corporation Ltd & ors -v- Quinn & ors* shows.

Predictive Coding is naturally gaining momentum, and it is estimated that around 90% of legal teams conducting document review are using it in some form.[1]

At the same time, the phenomenon of outsourced document review is gaining favour with legal budget holders and so legal services are being unbundled to enable instructed lawyers to concentrate on running the case. Predictive Coding plays an important role in helping lawyers to supervise this process, since the consistency of Predictive Coding can be used to evaluate the performance of lower-cost reviewers.

Whether Predictive Coding is used to fully categorise documents, as a quality control aid, or merely to prioritise the flow of documents in a review, the flexibility and benefits of this technology are steadily being proved to convince even the most reticent of legal teams that they can organise their document review projects more efficiently.

An extremely cost-and-time-effective method of review, the popularity of Predictive Coding is set to soar as it becomes more widely-understood by lawyers.

Strategic Case Assessment and Structured Data

Lawyers are now often looking for more value from their ediscovery providers, in the form of strategic, matter-specific advice that helps them find the most pertinent documents more quickly. Keyword searching, visual analytics, and granular analysis of the types of data that are located in different parts of a data set are tasks that have given rise to a new skill set. Ediscovery experts are now busier than ever helping lawyers to focus on the legal issues of the case. An expert in visual analytics can expose valid lines of inquiry from an overview of communications between individuals.

Such experts can also refine keyword lists accurately, based on detailed reports rather than guesswork. Concept searching, for example, identifies those words that are most commonly associated with words of interest. This enables lawyers to improve their search terms, and spot any code words that may have been used by key custodians – a feature that is particularly useful in competition cases.

Today it is also commonplace to examine structured data systems in the search for evidence. Systems which track stock, prices, customers, discounts and transactions for example, contain multiple millions of individual data entries that simply cannot be managed nor analysed without some computer power and the intelligence that goes with it.

But while the technology can retrieve relevant items of structured data, human intelligence is required to validate the results and piece them together properly. The smallest anomalies in structured data systems could help establish the most significant facts, but the process is more about assembling jigsaws than it is about needles and haystacks. It is necessary to understand structured data systems before attempting to preserve or search aspects of those systems. You need to understand the significance of the fields you plan to interrogate not only to know whether you have a complete data set and are running the correct searches, but also how to interpret and present the results in a helpful and accurate way.

Cost-Reducing Technology

The aim of all such technologies is to help lawyers build their clients cases effectively, comply with duties to produce documents to other parties and importantly to control and thereby reduce their legal costs.

The latest development in this trend focuses on managing the volume of hosted data which normally incurs cost in itself. Platforms now enable the review of documents in 'text only' format, which reduces data volumes significantly. The text version of a document is responsible for only around 10% of the hosted data volume, which is convenient for running searches to cull data in an early data assessment phase without breaking the bank. Non-relevant documents may be archived and relevant documents can then be reviewed in native and image formats, so companies have more control over the costs of data management.

Conclusion

Technology is rapidly evolving to help make the ediscovery process more accurate, less costly, and more targeted. The more advanced these technologies become, the greater emphasis there will be on ediscovery vendors to provide clients with more education, training and support. To that extent, ediscovery experts are taking the lead in shaping legal search strategies to comply with obligations in a timely manner.

By Hitesh Chowdry
Legal Consultant, Kroll Ontrack
hitesh.chowdhry@krollontrack.com

1 Irish Bank Resolution Corporation Ltd & ors -v- Quinn & ors [2015] IEHC 175

2 Based on services provided by Kroll Ontrack during 2014.

» Digital Forensics

» Electronic Discovery

» Award-winning Software

» Managed Review Services

» Revolutionary Onsite Solution

» Expert Consultancy

Your Global Ediscovery Partner

At Kroll Ontrack we specialise in providing innovative electronic evidence services to our clients across the world.

We provide legal technology services to help law firms, corporate clients and government and technology entities recover, search, analyse and produce data efficiently and cost-effectively. Our highly skilled legal and technical experts assist clients in multiple practice areas including dispute resolution, competition and regulatory cases.

For more information about Kroll Ontrack and its offerings please visit: www.ediscovery.com/uk.

+44 (0) 207 549 9600 | enquiries@krollontrack.com | www.ediscovery.com/uk

Kroll Ontrack®