CPI Columns
Europe

August 2021

E-Discovery & Competition Law: Inevitable Partners

By Mathieu van Ravenstein & Marieke Datema

Forcyd

E-Discovery & Competition Law: Inevitable Partners

By Mathieu van Ravenstein[1] & Marieke Datema[2]

The COVID-19 pandemic has further accelerated the use of technology and the prominence of electronic data, as well as having changed many companies' working practices (with more employees working from home). It is arguably now more important than ever to ensure that proper processes and procedures are in place to identify key documents when a company is faced with a competition law matter.

The collection and review of electronic data has largely replaced the traditional collection of hard copy/paper documents in competition law matters, and competition authorities have adopted increasingly sophisticated investigation techniques. As many competition law matters involve large volumes of data, electronic discovery ("EDiscovery") has become an inevitable and powerful tool for companies conducting their own investigations or being investigated by authorities. "EDiscovery" is the term used to describe the process of identifying, preserving, collecting, processing, reviewing, analyzing, and producing/presenting electronically stored information in an investigation or legal claim.

In this article we consider the main reasons why a company may benefit from using EDiscovery in the context of competition law.[3]

1. **Internal compliance**: When a company is made aware of potential anticompetitive conduct or wishes to conduct a competition law audit as part of its compliance program, the aim of EDiscovery is to identify, in an efficient and cost-effective way, whether there is any evidence of anticompetitive conduct and, if so, the scope and nature of this conduct. The company can the use this information to determine whether further steps should be taken to reduce the company's risk of incurring reputational damage, fines, and damages/compensation.
2. **To inform strategy, reduce possible fines or reputational damage and comply with requests in an investigation**: An internal investigation can take place as part of a compliance program, but can also be a reactive step that a company takes after it is made aware of a potential competition law issue following a dawn raid by a competition authority. In an investigation by a competition authority, using EDiscovery can help a company efficiently identify the evidence that it needs to help develop its case strategy (including whether it wishes to apply for leniency and/or engage in settlement discussions) and to stay one step ahead of the authority. EDiscovery is also a useful tool to help the company comply with data requests by authorities, such as requests for information in the context of a European Commission investigation. For companies applying for immunity/leniency, Ediscovery is crucial to help identify the evidence to be submitted to the authority that will add significant value. In this context, there is often significant overlap between a company's own internal investigation and the steps a company takes to satisfy an authority.
3. **To identify evidence to strengthen a company's case/weaken the other side's case**: In the context of competition litigation, often involving anticompetitive conduct that goes back several decades, EDiscovery is a powerful tool to help identify the particular evidence needed to strengthen a claimant's or defendant's case.

Dawn Raids

Increasingly Sophisticated Raids

While some authorities temporarily suspended

[1] Partner at Forcyd.
[2] Consultant at Forcyd and freelance antitrust/ competition lawyer.
[3] The use of EDiscovery in merger control is outside the scope of this article.

dawn raids or did not conduct dawn raids in practice in the early months of the COVID-19 pandemic, the world is increasingly (at least in theory) back to "business as usual" and authorities remain willing and able to conduct dawn raids.

The collection of electronic data has largely replaced the traditional collection of hard copy/paper documents in dawn raids. The procedures for collecting electronic data vary to some extent between authorities, but a consistent theme is that authorities are becoming increasingly sophisticated in their approach to searching, reviewing, and copying electronic data. Furthermore, the tools used by authorities may give them access to more data than if they were collecting paper documents. Companies need to adopt appropriate technologies to ensure they are not placed at a disadvantage.

Preparing for a Dawn Raid

Dawn raid preparation and mock dawn raids must now encompass training for appropriate members of the IT team in addition to addressing the classical issues (such as preparing reception staff, ensuring that appropriate legal team members are contacted, and appointing shadowers). IT team members will need to ensure that they have a detailed understanding of the company's IT environment; they must also have an awareness of authorities' rights and procedures and understand what their role would be in assisting inspectors with any IT-related issues (including blocking certain email accounts, temporarily disconnecting running computers from the network, providing administrator access rights support, etc.). This is especially important as, in many jurisdictions, companies can be fined if, in the course of a dawn raid, they fail to grant access to electronic data that is accessible from the relevant premises.

More generally, clear and transparent data governance systems will help ensure that data can be identified and collected efficiently, and a more coherent EDiscovery process. A company should also make sure that it has processes in place to suspend its routine document retention and destruction policies once an investigation or litigation is reasonably anticipated; it is also helpful to have considered how a legal/ litigation hold notice will be issued and drafted to ensure preservation of relevant documents.

What Types of Data can be Seized? Where and How can Authorities Search for This Data?

The European Commission can search the "IT environment" of the company it is investigating, which includes servers, desktop computers, laptops, tablets, and other mobile devices; it can also search "storage media" which encompasses a large range of devices with electronic storage, including servers, hard drives, mobiles, and/or tablets. The European Commission has also accessed cloud data stored remotely when conducting raids in various cases. The types of data examined by an authority are extremely diverse, and range from emails, Word and PDF documents to WhatsApp, instant messenger, and chat messages. Audio documents have also become increasingly important in investigations, with authorities able to review phone calls made from landline and mobile phones. Authorities are also able to access "meta data" which provides information about a document that can be particularly useful in a competition investigation including the author, the date it was created, altered, sent, accessed, or deleted.

Authorities will use various forensic IT tools to analyze the relevant electronic data; this includes search tools, but also EDiscovery software such as Nuix/Nuix Discover (used by the UK's CMA and the European Commission). These tools make it easier for authorities to search, identify, and copy large volumes of data; companies that are reluctant to adopt similar technologies will be placing themselves at a disadvantage.

As was recently confirmed by the European

Court of Justice, it is possible for the European Commission to start a raid at a company's premises and continue it at its own premises (provided procedural safeguards are observed) – this will be particularly relevant in cases where there are large volumes of data, but may become a more common practice in light of changing work practices due to the COVID-19 pandemic.

Asserting a Company's Rights in an Investigation

In any scenario, it is vital for a company to have internal and potentially external IT/forensic specialists available to work with legal counsel and clearly establish which documents inspectors are seeking to collect, and whether certain documents can and should legitimately be excluded from the collection process (whether immediately or in due course). The presence of IT/forensic and legal specialists is also important to ensure that procedures are in place to prevent employees from destroying or removing electronic and/or hardcopy evidence that may be relevant to an investigation; such conduct has led to several authorities, including the CMA in the UK and the ACM in the Netherlands, imposing significant fines.

A dawn raid is not a "fishing expedition" and the documents collected by an authority should be limited to those relevant to the matter being investigated (for which there must be sufficiently strong evidence); the search terms used by an authority must therefore be sufficiently precise. If possible, shadowers should try to take a note of any keyword search terms used by the inspectors when searching electronic data. This is increasingly difficult in practice, as authorities are using forensic search software in which at least some search terms are likely to be pre-programmed; this makes it difficult for those shadowing to identify precisely which search terms the inspectors have used.

In many countries, a company is not required to provide private and privileged documents (bearing in mind that the concept of legal privilege varies across countries) to an authority. Technology that includes personal data and privilege "filters" can help identify and exclude from collection documents that may be privileged or contain private data. Privilege filters will be especially important in some jurisdictions such as France, where the competition authority seizes entire mailboxes and then gives the company's lawyers a short timeframe to complete a privilege review. Separate procedures can also be used in respect of documents that are likely to contain personal data, such as the establishment of separate data rooms with limited access.

Next Steps… Launching an Internal Investigation

It is vital that companies have a clear record of the documents collected by the authority. The documents seized by the authority can provide a starting point for an internal investigation (or may supplement an existing internal investigation) and may also form the basis for interviews with employees to allow a company to better understand the nature and scope of the relevant conduct. As is discussed further below, an internal investigation is key to determining the company's strategy, bearing in mind not only investigations but also potential future damages claims. In cases with large data volumes and tight time frames, it is often beneficial to use a combination of predictive coding (Technology Assisted Review, "TAR") and manual review. Continuous Active Learning ("CAL") is a type of TAR and combines the best elements of manual review by skilled reviewers and technology; CAL prioritizes data in real time based on coding by reviewers/ lawyers, resulting in a prioritization of the more relevant documents in the review queue before the less relevant documents. Using CAL will often result in ultimately reviewing fewer documents because the more relevant documents will have been reviewed sooner, allowing for an earlier assessment of whether a specific type of conduct exists and its nature. CAL will also often be able to identify relevant documents that would not be picked up

by search terms alone.

Many authorities do not yet use these advanced technologies (or only use them to a limited extent), meaning that companies using them can quickly identify information that is key to determining their strategy and remaining one step ahead of the regulator.

Internal Investigations

Once a company becomes aware of a potential competition law breach (whether through a dawn raid or an internal complaint) and makes the decision to investigate further, what are the next steps? One way to obtain further information about the potential competition law breach, including how serious and widespread the breach may be, is to conduct a document review of key individuals' documents. A well-structured review of such documents can help inform a company's strategy, including: whether to apply for immunity/leniency, and/or to inform the company's defensive strategy in its discussions with authorities; what compliance training may be needed; and how to address potential breaches with relevant employees.

It is not uncommon for the scope of an internal investigation to be very wide because there is only a limited description of alleged anticompetitive behavior. This means that the material scope will be very wide in terms of the number of people involved and the timespan, often resulting in a very large population of documents to be reviewed. In order to make this process more efficient and less time consuming it is recommended to combine a manual legal review with CAL, for the reasons described above - it will often result in ultimately reviewing fewer documents, allow for an earlier assessment of whether a specific type of conduct exists and its nature, and may be able to identify relevant documents that would not be picked up by search terms alone.

It is vital to plan and structure a document review so that it can be run as efficiently and effectively as possible. Having a clear methodology for a review is important for internal purposes but also, if necessary, to be able to demonstrate (and defend) to an authority how the review has been conducted. Below we set out a number of high-level points to consider when designing a document review:

- Identify which (further) documents need to be reviewed and how to safely and securely obtain these, taking into account relevant local data protection, privacy and other laws and regulations; if a dawn raid has taken place, some documents will already have been identified and collected as being potentially relevant to the potential breach(es). This step will likely require conversations with key individuals in the company who have a feel for the relevant custodians whose data will need to be identified and collected. As is discussed further below, for some companies this may involve collecting and reviewing data from various sites and in numerous languages.
- Determine (i) on which platform the document review will take place (is there an internal document review system or will the company require an external provider?) and (ii) who will review the documents, bearing in mind languages and skills (should this be someone from e.g. the in-house legal team or an external provider?) and how many people will be needed for the review. The number of people needed to review documents will be influenced not only by the number of documents, but also by how quickly the documents need to be reviewed and the extent to which technology can be used to streamline the review (see below).
- Be clear on the aim of the document review and how the information coming out of the document review will be analyzed and presented, as this may influence how it is structured; bear in mind that this may change during the document review (for example, the initial aim might be to use a targeted internal document review to gain a better understanding on the nature and

scope of a potential breach in order to prepare compliance training, but this could change if a decision is made to apply for immunity/leniency). If documents will be provided to an authority, consider which types of documents can be excluded such as privileged documents and documents containing personal data.

- Consider the structure of the review; depending on the aim and desired output of the review it may, for example, be beneficial from a cost and efficiency perspective to have several 'levels' of review. This could involve (i) paralegals or more junior level lawyers carrying out the first-level review to determine whether documents are relevant or not relevant, and (ii) a second-level review (of documents coded as relevant at the first level) by more senior lawyers who may be more closely involved with the matter and can make a final judgment about how a document should be categorized and used. It is also worth thinking about whether some reviewers may need particular training before starting the document review; this could be competition law training, or training about the relevant sector that is the subject of the review.
- Develop a review protocol/guide that reviewers can use to help them correctly code documents. Depending on the nature of the review, this could be a guide which explains what types of documents are relevant/not relevant, or explains how documents should be categorized. Such a guide can include examples of the types of documents that would be categorized in a particular way.
- Consider which technologies can be used to streamline the review. In addition to the use of appropriate search terms consider, for example, whether CAL can be used. As mentioned above, this is a technique through which the document review system learns how to classify and/or rank documents based on ongoing coding by reviewers, which can often pick up more relevant documents than through the use of search terms. The extent to which certain technologies can be used will be partially influenced by the age and quality of the documents in the review (for example, generally speaking, it will be more difficult to use CAL if documents are older and of poorer quality). As discussed in the section below, email threading and content searching may also help to make a review more efficient.
- Consider whether there are certain types of documents that can be excluded from the review by, for example, using technology such as batch coding and/or personal data and privilege "filters." This can make a review more efficient by preventing reviewers from spending time reviewing many of the same types of documents.

Investigations by a Competition Authority

Once it becomes apparent that a company is being investigated by an authority for potential anticompetitive conduct, it is prudent to establish a document collection, review, analysis, and production process in line with the points set out in the "Internal investigations" section above. Even if a company decides not to apply for leniency/immunity, a document review process will still be needed to: (i) reply to requests for information issued by an authority (please see more on this below); and (ii) understand the nature and scope of the alleged anti-competitive conduct and, on the basis of this, allow a company to formulate its strategy in the investigation. The information identified during the document review can help the company determine, for example, if it will contest that the conduct was anticompetitive or if it is willing to engage in settlement discussions with the authority.

Applying for Immunity/Leniency

Following a dawn raid or an internal complaint or review, a company may decide to apply for immunity or leniency with the aim of reducing

its potential fine. There is significant time pressure associated with applying for immunity/leniency, as the company that provides evidence the quickest has the best chance of obtaining immunity, partial immunity, or a higher leniency band. While the exact obligations associated with being an immunity or leniency applicant vary by jurisdiction, it is generally the case that applicants must provide the authority with all relevant information and evidence relating to the alleged conduct and be available to promptly answer the authority's requests/questions. This will include supplying copies of relevant documents identified during a document review, as well as submitting statements (referred to as "corporate statements" in the context of European Commission investigations) which provide detailed descriptions of the conduct and additional insights into or explanations of documents provided by the applicant. To receive a fine reduction in a European Commission investigation a company will need to ensure that it provides evidence that adds "significant value" to the evidence already in the Commission's possession (other authorities also take a similar approach).

Applying for immunity/leniency is a weighty obligation that will require a company to set up and establish a comprehensive document collection, review, analysis, and production process (to the extent this hasn't already been established). The points set out in the "Internal investigations" section above will all be relevant, with special attention paid to ensuring that the documents collected and reviewed will meet the obligation of providing all relevant evidence and significant added value. In most jurisdictions, there are leniency "bands"; for example, for European Commission investigations, the first successful leniency applicant (after the immunity applicant) will receive a fine reduction of 30-50%, the second successful leniency applicant will receive a fine reduction of 20-30% and subsequent successful applicants will receive fine reductions of up to 20%. The quality of the evidence provided will influence the percentage reduction obtained by an applicant, which often equates to millions of Euros/pounds. For many companies, this will often mean spending time to map where relevant evidence may be found within the company and can involve collecting and reviewing data from various sites and in numerous languages. These factors will influence the structure and make-up of the review team (e.g. to ensure that reviewers speak the relevant languages) and, given that large volumes of documents will likely be involved, the technologies that can be used to make the review as efficient as possible. In addition to the possibility of using search terms, CAL, batch coding and data and privilege filters as mentioned above, other technologies that may be relevant include concept/conceptual searches and email threading. Conceptual searching draws documents together based upon the ideas and relationships of the documents. There are different ways conceptual searching can be applied; one way is that the platform can find conceptually similar documents to relevant highlighted text in a particular document. The platform then ranks the documents according to how conceptually similar they are to the content selected. Email threading identifies email relationships—threads, people involved in a conversation, attachments, and duplicate emails—and groups them together so reviewers can view them as one coherent conversation (as opposed to separate emails that may be reviewed by different reviewers).

Requests for Information ("RFIs")

Regardless of whether a company applies for leniency/immunity, it may be the subject of requests for information ("RFIs") issued by the authority. RFIs can range from more generic questions about company structure and names of relevant employees to more specific questions about certain documents (such as those seized in a dawn raid), specific meetings or dates. An authority may also request that a company provide documents in response to certain search terms that have been set out by the authority. At times the search terms set out

by authorities can be overly broad, so it is important for a company and its advisors to analyze the results of the searches and, if the results are too broad, to propose alternative search terms and/or methodologies to an authority.

It is crucial that companies are able to respond to an RFI accurately and in a timely manner. In a European Commission investigation, for example, significant fines can be imposed if a company supplies incorrect, incomplete or misleading information or does not supply information within the required time-limit.

The tight time limits often imposed in RFIs underline the importance of having taken steps to set up a document collection, review, analysis, and production process before an RFI is issued. Taking the time to set up these processes will make obtaining responsive documents easier and will also minimize the risk of providing inconsistent or incorrect information (it can damage a company's credibility if it, for example, provides different answers to the same or similar questions in an RFI as compared to its response to the statement of objections). In addition to developing and using appropriate search terms to identify documents responsive to an RFI request, other technologies that can be used include concept searches, email threading and TAR/ CAL. As noted above, depending on how many questions are contained within the RFI, it may make sense to have several levels of review: first level reviewers to identify documents that are responsive to the RFI questions and second level reviewers to further refine which documents should be provided to the authority and who may be involved in drafting the RFI response accompanying the documents.

Damages Claims

Follow-on damages claims have become increasingly prevalent in the last ten years and now follow (almost) every competition decision issued by national authorities or the European Commission. The damages claims issued all over Europe following the 2016 and 2017 European Commission decisions in *Trucks* are prime examples of this development. In July 2016, the European Commission reached a settlement decision[4] and imposed fines on several truck manufacturers (MAN,[5] DAF, Daimler, Iveco and Volvo/ Renault) in relation to their participation in a 14-year cartel relating to trucks pricing and the passing on of the costs of emissions technologies. In September 2017, the European Commission issued a decision[6] and imposed fines on Scania in relation to the same cartel (Scania had refused to settle with the European Commission). Since these decisions were issued, damages claims (some of which are collective/class actions) have been issued against the truck manufacturers in several European countries, including the UK, The Netherlands, Germany, Spain, and Italy.

In follow-on claims the anti-competitive conduct has been established by an authority and the key element of the claim is quantifying the (alleged) damage caused to a claimant. There are also an increasing number of "stand alone" competition claims in which there is no decision on which base the claim and the alleged anti-competitive conduct must be established by the claimants.

Many of the same aspects of EDiscovery discussed above in the context of competition law cases are relevant in damages claims, on both the claimant and defendant side. In England, for example, in follow-on damages claims, there are often several rounds of disclosure relating to, amongst other issues, the value of commerce, interest, overcharge, passing-on and the European Commission file (i.e. the evidence gathered by the European Commission in relation to the cartel). Given that many cartels last a number of years, there will

[4] https://ec.europa.eu/competition/antitrust/cases/dec_docs/39824/39824_8750_4.pdf.
[5] MAN was not fined as it was the immunity applicant.
[6] https://ec.europa.eu/competition/antitrust/cases/dec_docs/39824/39824_8754_5.pdf.

often be large amounts of data that need to be identified, collected, and reviewed. English courts generally expect parties to use technology to make the review of large volumes of documents more efficient unless there are valid reasons for not doing so.

When reviewing the Commission file in a follow-on claim, the evidence that claimants will seek to find is more specific than what a competition authority or a leniency applicant would have looked for. Whereas a competition authority/leniency applicant will have sought to identify evidence of an infringement (including its nature and scope), in damages claims, an infringement has already been established; a key focus in damages claims is therefore to identify documents that can help to build a claimant's case and demonstrate *how* the anti-competitive conduct caused damage e.g. by increasing prices for customers. On the defendant side, a key aim will be to identify documents that suggest that the infringement did not actually cause damage to customers. Technologies such as CAL can be used to more efficiently identify documents that are key to building a claimant's or defendant's case. However, in cases relating to long running cartels, a large number of documents may be very old (from the 1980s or even earlier) meaning that the quality of documents may be very poor (e.g. hardcopy documents that have been copied several times over); this may make it difficult for technology to properly "read" the documents and identify similar ones. In this case, a manual review may be needed for certain older documents.

Conclusion

Regardless of the reason why a company engages with EDiscovery, whether driven by internal compliance or by a specific request from a regulator, there will be an assessment to determine if and to what extent time and money should be invested in the EDiscovery process. This assessment will often consist of a balancing act between the perceived likelihood of damage being caused to a company as a result of potential anticompetitive conduct and a willingness to spend resources upfront to ensure that a company gets on top of the evidence as efficiently as possible and can use this to inform its strategy. This can be a difficult assessment to make, especially for companies who have limited experience of EDiscovery; such companies may benefit from speaking to experienced practitioners who can provide practical examples to highlight the benefits of using EDiscovery.

EDiscovery plays an important role in various types of competition law matters. In particular, taking the time to plan and structure how documents will be collected, reviewed, and used can play a crucial role in informing a company's strategy and response to alleged anticompetitive conduct. Many competition law matters involve large volumes of data and the intelligent use of various technologies, including CAL, data and privilege filters, batch-coding, concept searches and email threading can make a competition law matter run more efficiently and make the matter more manageable for a company and its employees.