CSI ANTITRUST

Modern cartelists are using increasingly sophisticated technology to elude detection. Forensic investigators are raising their game in response. Lewis Crofts reports

Illustration Lisa Smith

I would love to know what is on your laptop. It wouldn't take much to find your holiday snaps, the illegal copy of *The West Wing* (series four), and that e-mail where you and Jean-Paul argue about who is going to pick the kids up from school. But you'll hope there's stuff I won't find. After all, you deleted it ages ago, didn't you? You used Gmail, not the company mail account. You didn't open the attachment. You weren't online at the time.

However, you're not particularly worried about me, are you? The worst I can do is laugh at that video of you falling out the hammock at your holiday house. I can't force your employer to pay more than a billion euros in fines. I can't disqualify you from holding a decent job for a few years. But somebody else can. And they can find the data as well.

The Golden Age

There was a time when price-fixing was easy. You met your competitors in a hotel (the Sofitel in Munich was always comfortable). David booked a conference room. Sven checked for cameras. Pedro ordered the food. You scribbled down a few notes (don't forget: 102 francs per tonne) and then headed back to your office, put your feet up and watched that market-share remain impervious to the commercial buffeting of free-market winds.

It was easy for the cartelists. But it was also easy for the cartel-busters. Former antitrust officials testify that in that golden age they would turn up unexpected at a company under suspicion, walk in past reception, go to the sales manager's office and look in his top left drawer. And there it was staring back at them: the headed note-paper from the Munich hotel.

Now, though, there is technology. Cartels are more sophisticated. They feature throwaway mobile phones; private e-mail addresses accessed from home;

instant messenger services, and perhaps even social media. Old-school cartels are not dying out. Last month, an EU court heard how one cartelist had conveniently used company notepaper to document cartel-meetings. Still, cartel members are getting wiser. Some of the most complex antitrust investigations are into the world's largest banks and their suspected manipulation of lending rates and credit default swaps. In such cases the smoking gun is unlikely to be an incriminating note on Goldman Sachs notepaper.

"The question is whether the cartel enforcers can stay ahead of more sophisticated cartelists," says Peter Camesasca, a Brussels-based lawyer. "There will always be some smoke-filled rooms, but these will be fewer and fewer. As the European Commission becomes more successful, cartel members will go deeper and deeper underground."

Dealing with data

Companies involved in price-fixing are often vast enterprises whose fingers stretch round the globe. And this means their data does as well. They may have servers in Manitoba and Madagascar. They will have employees using smartphones in Cape Town and Singapore. And there will be backup systems in the 'cloud.' So, when antitrust officials come calling, it can be difficult to access and collate that data. This means that everyone has had to raise their game: both the hunters and the hunted. And in the middle are their technical consultants trying to find an efficient way to plough the data fields, alongside their lawyers making sure it doesn't undermine their legal case.

"Data volumes are increasing exponentially," says Tracey Stretton, legal consultant at Kroll OnTrack, a company offering e-discovery and computer forensic services. "There is more data and more demand for e-discovery services in antitrust investigations in Europe." She explains that in raids, "multiple terabytes" of information can be collected and that companies are using intelligent technologies to handle it. To most of us, a terabyte means about 1,300 CDs or around 200 DVDs. To a company, it means a headache.

When antitrust officials visit a company they can only seize copies of documents, not the originals. For data, this means making entire images of hard drives. It can take days to go through this evidence to find the files covered in cartel fingerprints. So, they put the copied drive in an envelope, seal it and take it back to Antitrust HQ to search in peace, with the company's lawyers looking over their shoulders. Afterwards, it is destroyed. This is the European Commission's approach and it is replicated in many EU countries.

However, European antitrust law says that officials can only seize "relevant" data. You could argue that a hard drive that contains everything from your holiday snaps to your music collection is jam-packed with irrelevant information for an antitrust official. "A few years ago a laptop would have up to four gigabytes, now a standard hard drive can have up to 500 gigabytes," says Sandeep Jadav of

When antitrust officials visit a company they can only seize copies of documents, not the originals

Ernst & Young's fraud investigation and dispute services department. An e-mail archive of 60 gigabytes might contain up to 600,000 separate documents. "The amount of data is huge," Jadav says.

Regulators could argue that it is more efficient to copy the entire drive, rather than squat for three weeks on company premises scouring every file. Crucially, most companies agree. The first thing they want during a dawn raid is to get it over with and to bring the investigators back to Brussels, Paris or London.

Yet, investigators are sometimes accused of "fishing" for other information, essentially casting their net as wide as possible, snagging all sorts of conduct which they were not authorised to find.

The idea of 'relevance' is yet to be tested in court, but companies involved in a current EU investigation of a suspected undersea-cable cartel have gone to the General Court in Luxembourg to argue that the European Commission was not specific enough in its search. While the commission should be free to follow up on well-founded suspicions, companies will always try to ensure that those are as narrowly defined as possible.

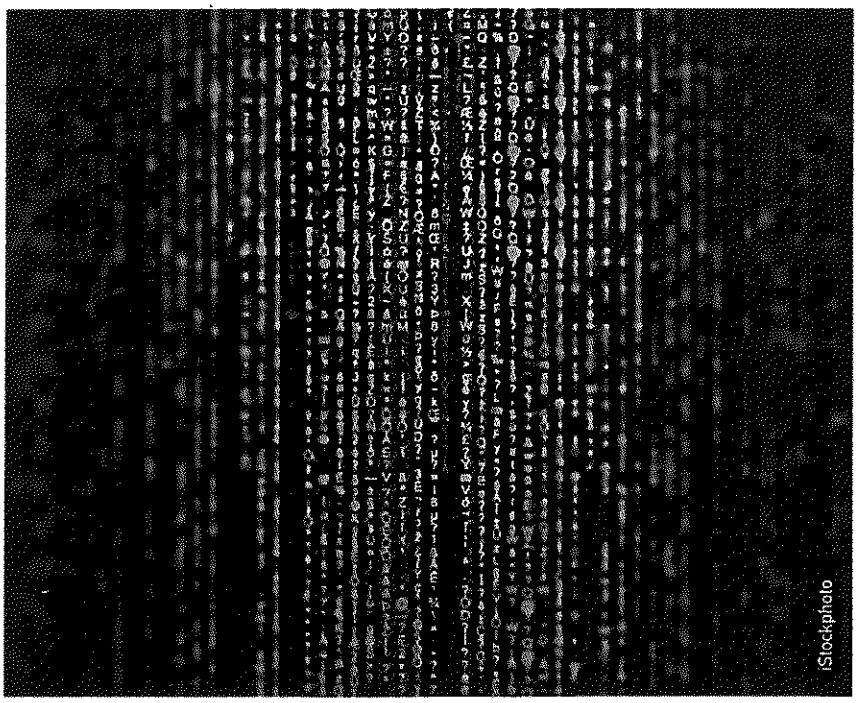
"There is a real risk that regulators will be swamped by data and they have to strive to get on top of it more quickly than the companies, and all within the confines of a budget," Kroll's Stretton says. "Some of the data requests that are coming in indicate that the regulators are getting on top of their game. There is an increasing level of expertise. You can see that from the search terms they are setting."

In the UK, the Office of Fair Trading enjoys similar powers to take 'relevant' information, but it also benefits from the Criminal Justice and Police Act, which grants 'seize and sift' powers. Essentially, this means it can take irrelevant data and then sort out the wheat from the chaff. It can also visit private property, which it did in an investigation of a marine-hose cartel.

But regulators argue that the accusation of a 'fishing expedition' is unfounded. Cartel raids are often conducted after one of the members has blown the whistle on the conduct, so officials may have a decent idea of who is involved, what codenames have been used, and when the meetings took place. While they will never close their eyes to other data they happen upon, frequently they already know what they are looking for.

Capacity

The European Commission is expected to be sophisticated: it has cohorts of antitrust officials investigating some of the most egregious conduct. But local cartels are becoming more sophisticated as well, and this raises questions for national antitrust agencies. For example, in Portugal, the legal situation is more unclear. "Competition law infringements are legally misdemeanours, not crimes,



Incriminating stuff

which means investigative tools are more limited than for the criminal police," explains Miguel Mendes Pereira, a partner with Vieira de Almeida Pereira in Lisbon.

For example, the antitrust regulator would not be allowed to access unopened mails. Legally, it is tricky to "interfere" in communications in Portugal and this is "not done lightly," Mendes Pereira says, adding that it is a "politically very sensitive issue."

A planned reform of the law should allow the competition authority to target such data, meaning that its activities in forensic searches may soon expand. "The agency is taking e-discovery very seriously. It is aware of the critical role of forensics and it is increasing its capabilities." But Mendes Pereira warns that with greater power comes greater responsibility. The new law shouldn't allow the regulator to "recycle information from one investigation into another," he says.

Ingo Brinker, a partner with Gleiss Lutz in Munich, says that the German authority has "also been very successful in increasing its capacity," pointing towards the employment of specialist IT consultants. "The learning curve has been very steep," he says.

But still all eyes are on the European Commission. A couple of years ago, EU officials were said to be well behind the companies they were trying to prosecute, now they are "rated very highly," according to one lawyer. "They have come on leaps and bounds in hardware and software," says another. "They have power I've rarely seen before. Whatever you had on a server before, even if it has been deleted, they'll find it."

There are a handful of specialist IT data-crunchers in the Brussels HQ, and a wider team of cartel officials trained in the dark arts of forensic data gathering, who are called upon when dawn raids are co-ordinated across several countries. The core team and the software at their disposal is said to be "on a par" with some of the corporate players. But where they fall down is arguably in sheer manpower.

With data there are two key phases: collecting it, and analysing it. The first part can be done efficiently by software, which will pull the 0s and 1s off servers and index them into a half-usable format. Then comes the difficult part, navigating it to find what you're looking for. Large corporations or specialist services such as Ernst & Young, AlixPartners or Kroll OnTrack have the capacity to throw numerous specialists at the data set and conjure up answers.

Regulators, subject to budgetary constraints, rarely have that luxury. EU officials may end up asking company representatives to point them to the pertinent parts of the server for the information. A company could, of course, be less than forthcoming, but then it might face nasty sanctions for failing to co-operate. So, trust plays a role. EU officials will still conduct random searches of other parts of the system and take a broad look at the IT infrastructure, but they won't be able to turn over every stone. That would be unrealistic and impractical.

"There is a risk that regulators are too focussed on what the forensic searches turn up," says Kristian Hugmark, a partner with Swedish law firm Vinge. He warns against an "over-reliance" on the results of search terms. "You should also look at the structure of the systems, and once you have a hit, look around it, get the bigger picture." While cartel-busters may come across strong evidence of a cartel, they could be missing documents that give "vital context," he says. "The human touch will always have a role: old-fashioned lawyering and detective work."

Lawyers follow EU officials every step of the way when hard drives are being sifted. Later, they will go back over each step and note down what the investigators found, trying to get a feel for the evidence held against them. More often than not, they discover that the commission has missed something.

Regulators certainly have more limited resources than corporations, but there are services and software that can lighten the load. So-called 'intelligent review technology' combines the skills of lawyers with the processing power of computers, allowing software to learn how relevant a document is. It will then naturally push the more relevant documents – say, those featuring certain coded terminology – to the top of the pile.

Structured vs. unstructured

It is in the world of 'unstructured' data where forensic skills are really brought to bear. 'Structured' data refers

to hard information such as sales and purchasing statistics, or accounting figures. If you look at these, you may find that on Tuesday afternoon at 3.00pm, across a group of competitors, the price for a particular product spikes. This information can then be "mapped across" to 'unstructured' data such as internal communications, Bruno Augustin from Ernst & Young explains.

"The effects of certain e-mail traffic on trades can be demonstrated," Augustin says. "A lot of cases have a smoking gun, but then you need to see the context, build up a set of connections and establish the causality." The price spike in a financial product could, for example, be linked to e-mail traffic between the same three traders at different banks, all sharing a code word. Such 'unstructured' data can be crucial to building a complete picture if you are a whistleblower. Or, if you are a defendant, the same data could be crucial to rubbishing the regulator's case.

The more we move from personal computers to mobile devices, data becomes less structured and potentially spread across smartphones, tablets, home computers and a variety of servers. Ernst & Young's Sandeep Jadav says there has been a "change in practice." A typical executive might have one device for work and another for private calls. Some devices are also quite insecure, from a data perspective. This raises the question of what is personal information and what is corporate information, he says. But, for regulators, if they believe the device is used for anticompetitive practices then they will try their best to seize its data.

"Social media has changed the game," says Steve Ambort, managing director of AlixPartners, who leads the forensic technology practice in Europe. "While people are obviously increasingly aware that e-mails are stored for a long time, they aren't as aware that many of their communications on social media sites are tracked and retrievable as well."

"Employees, intentionally and unintentionally, are creating a record of communications and activities on social media sites such as Facebook, Twitter and LinkedIn that may be relevant in future investigations or litigation disputes. Although these types of communications are off the grid of corporate IT departments, they are still possibly building a record of evidence for future legal cases."

Indeed, information shared over social networks such as Facebook or Twitter has also been used in US litigation recently. "E-mail is dying out," says Stretton from Kroll. "BlackBerry messenger and text messages, for example, are used more frequently. Some people think they can't be obtained but they are being used as proof of, for example, cartel behaviour."

Recent antitrust investigations in the financial services area are said to have seen potential collusion taking place over Bloomberg's messaging system as well. One court document filed by the Canadian authority indicates that an individual involved may have been named 'Colin.' It struggled to find more than that. And what does all this mean? The data the regulator wants might not be held by the company, but elsewhere, on servers owned by Google, Vodafone, Bloomberg or Amazon.

With the advent of cloud computing, data of potential interest to the commission might be stored far beyond Europe

In last summer's riots in London, the police believed that looters were communicating via BlackBerry Messenger and then sought disclosure of the information from the company's servers. However, while that concerned criminal prosecutions, it might be more difficult in an administrative procedure.

Cloud surfing

This is part of a much larger issue: what can a regulator do when data is held elsewhere? With the advent of cloud computing – where companies don't own their servers but rent server space from larger providers, often in other countries – this can mean for the European Commission that potential data is stored far beyond the borders of Europe.

"Cloud computing is a tricky area in regulatory investigations and litigation," says AlixPartners' Ambort. "While cloud storage may provide convenience and cost savings, these benefits can become a hindrance in the context of investigations and litigation, where one is trying to extract and filter data. We are finding that data stored in the cloud can be much more difficult to extract, compared to data sitting on one of the company's servers. But it is still early days."

He says that cloud computing has proved to be a sound idea for storage, but these systems were not designed to access information in urgent enquiries or to extract large data sets. "It is giving us more headaches than we expected," he explains. "How do you get the information you want quickly and in the right form? You may know where it is and who the vendor is that stores the data, but in our experience, getting the data out of the cloud can be an arduous process."

While the companies may face those issues, for the European Commission the approach is more straightforward: anything that can be accessed from the company's computer can be copied by the officials. So, if they raid an office in Bratislava, it doesn't matter if the company data is kept in Alaska. If the employee can access it, then the inspector can take it.

But it does raise the question of where Europe ends. If a Japanese manager is writing an e-mail in Japanese to a colleague, across a Tokyo-based server, it could still land in the hands of EU officials, if that can be accessed from a London computer.

There are some limits. EU officials can only take data accessible during the 'normal course of business.' So, if the company happens to keep entire backup servers, accessible only to the IT staff, then these may not fall under that heading. However, this provision has never been tested in court, so no-one has yet argued against it. A regulator might argue that even backup servers for accounting information are

Gone, but not forgotten

part of 'normal business.'

"To get information from non-EU servers, you face an immediate problem: possible lack of jurisdiction. To establish jurisdiction based on the 'effects doctrine' and persuade the provider to co-operate, you will need to present a very detailed account of what you want," Mendes Pereira says. "However, it is unlikely that a competition authority will know precisely what they are looking for."

European antitrust regulators are presumed to have not yet asked any large non-EU cloud-service providers to hand over data held on a cartel suspect. Why? Usually, companies under investigation are more inclined to co-operate than to contest. Second, despite the technological Babylon of multiple devices in multiple places, more often than not a trace of the relevant evidence is left behind in an accessible place.

"People are more aware that e-mails are stored and data is stored so they switch to alternative methods," Ambort of AlixPartners says. "They are taking communications off the grid, but they are retrievable."

The key for many regulators is not to look at text messages or online chats as anything other than documents. If they are documents, then they must be disclosed, end of story. However, there are questions over what constitutes such a 'document.' In an e-mail, for example, would it be an excerpt, or the entire trail?

Data protection is a hot topic for parliaments around the world and regulatory regimes are cropping up where it may become increasingly difficult to obtain data. Ingo Brinker of Gleiss Lutz refers to strict data rules in Germany and France, as well as Switzerland.

"If a company has a Swiss subsidiary, there is legislation which makes it difficult to provide information outside of the country," he says. Brinker also notes that in Germany, for a firm to reveal data it may have to check with employee representatives first. This could heighten the risk of unwanted disclosure, which may undermine a company's attempts to put together a convincing whistleblower application.

Some in the industry note that companies are often calling for specialist services ahead of any antitrust problems. They see the value in establishing a data strategy in advance and getting a grip on how to react to a raid or litigation. Nevertheless, this remains a desire which many companies espouse but don't get around to paying for during peacetime.

Forensic services in the antitrust world are still in their infancy, although they are growing fast. While the US is at the forefront with the UK close behind – both are accustomed to e-discovery services through their litigation industries – the EU is snapping at their heels. Some expect antitrust regulators to take the lessons from forensic science in antitrust raids and apply them more broadly over time.

"If you are going to use these tools, then you might as well seek to apply them in other areas," Peter Camesasca says. "You could use the search tools to track price changes or industry behaviour. It could be used for broader monitoring of markets and economies."

The new front

Earlier this year, the heads of both the UK and US antitrust agencies said that building their capacity to deal with data was one of the largest challenges for their authorities. At present, most are praised for their advances, but they will face a struggle to stay ahead of the curve. Notably, a UK prosecution of British Airways executives for cartel conduct collapsed in 2010 after a trove of e-mails was not made available to the defence. This showed the importance of solid forensic work.

The Dutch regulator has also been praised for its approach, while the Belgian agency has called for more authorities to share their expertise and establish common principles. Faced with corporations growing in sophistication and often with bottomless pockets, they will need all their skill and expertise if they are to catch 'Colin.'