CARTEL INTEL

INTERVIEW WITH **ASHLEY BRICKLES**
SENIOR MANAGING DIRECTOR AT FTI CONSULTING

The cartel crackdown continues across EMEA, with levels of enforcement exceeding those witnessed immediately before the COVID-19 pandemic. Leading the way, the European Commission has conducted new dawn raid inspections in each of May, June and July. At the same time, the rules of the game have changed: the nature and scope of dawn raid inspections are evolving and businesses must act now to keep pace.

In advance of the next edition of *Cartel Intel,* **Daniel Vowden** (Partner, Brussels) discussed with **Ashley Brickles,** (Senior Managing Director at FTI Consulting) the changed nature of dawn raid inspections, the new tools and technologies available to antitrust authorities, and the precautions businesses should sensibly be taking. **FTI Consulting** is a market-leading global consultancy that has assisted clients with many of the world's largest, highest-profile antitrust investigations. Ashley Brickles has acted on some of the most demanding European cartel cases in recent years and specialises in solving data-related challenges that arise during these complex, multi-jurisdictional investigations.

The forthcoming edition of *Cartel Intel,* Herbert Smith Freehills' quarterly update on key EMEA cartel developments, will be published in August. It will be available, along with former editions, **here.**

DANIEL VOWDEN: Given the practical challenges and altered patterns of work resulting from COVID-19, what changes have you seen in the conduct of dawn raid inspections by the European Commission, as well as other competition regulators?

ASHLEY BRICKLES: Just as the workplace has entered a new era, so too have the global rules and processes around dawn raids. As you mention, working practices have changed dramatically: employees are now working from anywhere, storing data on personal devices and communicating across numerous chat, collaboration and video conferencing tools. As regulatory enforcement escalates, antitrust authorities have been quick to pivot their approaches to align with the modern data landscape.

It follows that there's been an increase in the practice of 'hybrid' dawn raids that includes raids at individuals' homes, collection of personal devices, virtual inspections, and more scrutiny on the data stored in collaboration applications and cloud-based systems

That's interesting to understand and is consistent with our recent experience at Herbert Smith Freehills. In the same vein, the Director of the European Commission's Cartel Directorate, Maria Jaspers, recently told the 2022 ABA Antitrust Law Spring meeting that the Commission expects to make greater use of its power to inspect domestic premises (it has since been confirmed that the European Commission has made successful use of this power in practice).[1] Michael Grenfell, the Executive Director of Enforcement at the UK Competition and Markets Authority ("CMA"), has also publicly warned of more home raids.[2] Given this trend, what should companies be doing to prepare their personnel for "home raids", including in terms of their mobile device management systems and access policies?

Just as you say, most experts in this space expect to see a marked increase in raids conducted at domestic premises over the months and years ahead. In some jurisdictions, such as France, regulators have long had the power to raid individual homes but, in practice, have only recently begun exercising these powers.

Other agencies, like the CMA, are looking to expand the scope of what circumstances and practices allow for home raids.

Organisations need to understand their IT data footprint and the full scope of where employees are storing data, as well as the apps and devices they use for work purposes. Bring your own device and other acceptable use policies should be revisited to account for the possibility that employees will be asked to turn over their personal devices during a raid.

The combined effects of digitalisation and the new, widespread reliance on remote working have led to an explosion in the use of cloud-based platforms, video conferencing tools and collaboration applications, such as Teams and Zoom. To what extent are antitrust authorities examining these data sources during dawn raids and other antitrust investigations? How should companies prepare for this?

1. Comments by Maria Jaspers on 5 April 2022

2. Speech by Michael Grenfell on 11 May 2022, "The CMA in turbulent times - where we are and where we're going" (available here).

These tools all fall within a category that we classify as "emerging data sources". Given the state of the modern workplace, most corporations now have an environment in which millions of documents are stored in dynamic formats in the cloud or third-party systems. Potential evidence of anti-competitive activity may reside in video conferencing applications and audio files, meeting transcripts, metadata from meetings, participant logs and more.

This is incredibly challenging for regulators, but also for organizations working to prepare for a potential dawn raid. In the work that we do at FTI, often in conjunction with firms such as Herbert Smith Freehills, emerging data sources are creating challenges across governance, privacy, compliance, e-discovery and investigations. Traditional work-flows across all these functions must now shift to accommodate the challenges and technical nuances involved with short-form messages, dynamic cloud files and multimedia formats like audio and video.

That's interesting to understand. On a related point, what impact are algorithms and artificial intelligence having on the way that antitrust authorities use data to identify and analyse anti-competitive practices?

Enforcement agencies are beginning to recognise the value that AI, data enrichment and data scientists bring to antitrust enforcement. For example, the CMA now has a director of data science who has said his group is helping the agency be more efficient and insightful with the large volumes of documents and other electronic evidence it receives.[3] The U.S. Department of Justice, authorities in Sweden and other jurisdictions are increasingly adopting AI tools and hiring teams of data scientists to enhance their reviews. To that end, the DOJ's head of the Antitrust Division has said: "[a]*s enforcers, it's extremely important that we're investing in the technological expertise, the data science expertise, to understand, to detect, to investigate and ultimately to prosecute crimes.*"[4]

Expanding on this further, how can both companies subject to dawn raids and competition authorities use new AI tools and analytics to interrogate data seized during an inspection?

In the same way that enforcement agencies envision using AI and algorithms to enrich data sets, organisations and their legal counsel can leverage a variety of AI and data algorithms to sift through large volumes of data to identify the key facts. At a more granular level, these tools can uncover clues within metadata, provide a clear view into potential infringement issues and develop crucial fact patterns in the aftermath of a dawn raid inspection. Some AI tools allow for communication mapping, where counsel can examine a group of individuals and figure out who they are most frequently talking to, when they are talking and develop a network of their key connections. In a cartel investigation, that's critical to understand who is speaking to whom and when that's occurring. Certain analytic models can also isolate themes that may suggest anti-competitive behaviour.

In light of the comments above, how can businesses use AI and analytics to strengthen their readiness for future dawn raids and investigations? For instance, is it possible to use such tools to monitor for indicators of competition law non-compliance or else to support data retention practices which can preserve and make readily accessible vital evidence?

AI provides some very interesting capabilities and use-cases for compliance monitoring. Advanced tools now provide sophisticated sentiment analysis and behavioural analytics that can uncover patterns in behaviour and escalate suspicious activity before it becomes a significant compliance violation, to the extent permitted by local privacy laws. For example, these tools can identify when employees are 'channel hopping', i.e., moving from written communication to phone calls to chat messaging platforms. Identifying these patterns provides valuable insight into potentially problematic conduct and helps focus early efforts when a broader investigation is deemed necessary.

Transactional data can also be used to proactively identify pricing patterns that may indicate collusive behaviour. Many times, monitoring can be done using existing data and internal systems, such as enterprise resource planning (ERP), customer relationship management (CRM), and business intelligence systems.

Moreover, organisations can enhance their data retention practices by leveraging key terms, metadata and analytic models to identify and classify different types of data (eg, invoices, contracts, policies, etc.). This allows for a more tailored retention policy that helps mitigate the risks and costs associated with long-term data storage practices.

In your experience, what other technology considerations do businesses need to address when collecting digital evidence during (or after) dawn raids or when replying to a regulator's requests for information?

Legal and compliance teams must implement thorough escalation and data access plans to enable the quick retrieval and export of electronic files requested by inspectors. This includes updating existing data use policies, performing high-level mapping exercises to understand where their data currently sits, and developing processes to reduce the risk of delays arising during a hybrid dawn raid where data may need to be collected virtually at an employee's home or retrieved from third-party or cloud-based systems.

Herbert Smith Freehills and FTI Consulting provide expert, individually tailored assistance on the increasingly complex legal and practical issues relating to dawn raid inspections and effective competition law compliance. Queries or requests for additional explanation on any of the topics touched on above can be directed to either Daniel Vowden or Ashley Brickles, or else your regular contacts at either Herbert Smith Freehills or FTI Consulting.

Our quarterly update on cartel developments, Cartel Intel, is available here.

KEY CONTACTS

Daniel Vowden
Partner, Brussels
T +32 477 883 438
daniel.vowden@hsf.com

Ashley Brickles
Senior Managing Director
T +44 20 3727 1066
ashley.brickles@fticonsulting.com

Updates and expert analysis on cartel and other key antitrust developments are available at HSF Competition Notes.

3. *See* "CMA using data science to screen evidence", Global Competition Review, 16 June 2022 and CMA Data, Technology and Analytics Conference 2022 (available here).

4. *See "Antitrust Division investing in technological expertise to address AI collusion"*, Global Competition Review, 5 May 2022.