ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

As EU Antitrust Enforcement Intensifies, Data Challenges Dominate

Compliance and Ethics

Banner artwork by Diyajyoti / *Shutterstock.com*

In the sphere of antitrust regulation, there’s near unanimous agreement that recent escalation in enforcement activity is only the beginning of what will become a groundswell of regulatory investigations and interventions. Under the European Commission’s jurisdiction, the rate of prohibition decisions in merger clearance has increased, the number of deals subject to remedies has grown and the power of national competition authorities has expanded. Likewise in other areas of competition enforcement, authorities are highly focused on pursuing cartels and abuse of dominance,

with a recent surge of judgements and newly opened cases.

In turn, general counsel and other leaders are increasingly concerned. A global survey of senior legal and compliance professionals found that one-third ranked the ability to remain in compliance and respond to regulatory inquiries as one of their top three biggest risks. More than 75 percent said they expect more regulatory investigations in the coming year and 30 percent expect their overall compliance risk to increase.

These concerns are already manifesting in real world matters. For example, in March 2023, the Court of Justice of the European Union made a landmark ruling that non-reportable transactions may still be subject to abuse of dominance rules. This ruling set a precedent that authorities in member states may assess deals not otherwise subject to merger control for abuse of dominance, which may lead to unexpected investigations, sanctions, or in severe circumstances, post-closing reversals. Moreover, the ruling suggests openness to investigate deals that in the past would not have been scrutinized.

Below the EU threshold but still scrutinized

In other activities, the Commission and member states are invoking Article 22 to monitor transactions that, while below the EU threshold for merger control, meet the threshold of one or more member states. There have been at least four recent instances of this trend, and more are expected in conjunction with guidelines in the Digital Markets Act.

In parallel to ramping enforcement activity, there has also been a widespread and persistent surge in the volume and variety of emerging data types (i.e., data from chat tools, collaboration applications, and cloud-based systems) coming into scope in these investigations. Moreover, the rates of growth and change across corporate data environments are increasing rapidly. Employees are using personal devices and apps, such as WhatsApp and Signal, to conduct business communication across every region, and the United Kingdom is the third largest market (behind the United States and China) for adoption of collaboration software.

> In parallel to ramping enforcement activity, there has also been a widespread and persistent surge in the volume and variety of emerging data types (i.e., data from chat tools, collaboration applications, and cloud-based systems).

Anecdotally, more than one-third of data now managed for legal and regulatory purposes falls within the emerging data category, up nearly 20 percent from the previous year. While in 2019 only roughly 10 percent of regulatory investigations included emerging data sources, today they all do.

Data creates unprecedented challenges

In an environment with highly active and stringent competition enforcement, data is creating an array of unprecedented challenges for organizations faced with responding to merger control inquiries, preparing for dawn raids and fulfilling the requirements of high stakes antitrust investigations. Key issues include:

Regulators have indicated a strong willingness to seize new data sources and formats.

Corporations that aren’t already aware of this fact need to appreciate that communications and documents within their chat and collaboration tools are now subject to investigation if a matter arises. This may include data on employee personal devices, which further complicates the process of accessing and collecting information, both from technical and data privacy standpoints.

New data sources including employee personal devices are subject to investigation if an issue is raised. Billion Photos / *Shuttterstock.com*

> Corporations that aren't already aware of this fact need to appreciate that communications and documents within their chat and collaboration tools are now subject to investigation if a matter arises.

The Commission is also reassessing Regulation 1/2003, which empowers inspection and seizure of data. Anticipated changes include potentially expanded powers for regulators to probe new sources of data.

Subsequently, these developments have led to an increase in the frequency and complexity of nuanced conversations with regulatory agencies around issues like how emojis, linked content, and document versions are handled in investigations, as well as whether and how cloud backups can be accessed if potentially relevant data has been deleted from a custodian’s device.

Agencies are bolstering their own internal data expertise.

There were several notable moves in this direction in the US last year, including the Department of Justice’s appointment of a data analytics and global compliance expert to an advisory position within its fraud section. Across Europe, regulators have amplified their analytics and investigations toolkits (albeit with commercially available technology, rather than bespoke solutions) to enable more robust

seize and sift capabilities for complex data. This is creating somewhat of a race for corporations to enhance their ability (and access to expertise) to properly handle and contextualize emerging data sources ahead of regulatory intervention.

Analytics have become essential.

As authorities become savvier and more rigorous about investigating all forms and sources of data, advanced analytics are becoming increasingly important in workflows for investigations, document review, and compliance. With sophisticated analytics, and experts who understand how to use them in complex situations, organizations can more effectively navigate regulatory matters. This includes responding to dawn raids (which may be conducted on-site, at employee homes or virtually), understanding fact patterns relating to competition issues, identifying relevant information across numerous languages and narrowing in on key individuals of interest. Analytics can also strengthen proactive compliance programs, which may support leniency applications.

There’s a rise in the exchange of information between agencies.

Increasingly, authorities are collaborating on antitrust enforcement across jurisdictions, including joint dawn raids, cross-agency response to whistleblower allegations and sharing of information between agencies. This includes collective efforts to scan markets, data points, and the internet for signals that may indicate anti-competitive behavior.

Expertise is essential in handling these issues, and the sophistication of approach has a direct impact on the ultimate time, cost, severity, and success of response.

For example, in one recent matter, FTI Technology supported a corporation and its law firm in conducting an internal audit that required review of messages and files within the company’s Slack environment and other complex data sources.

The company simultaneously engaged our team to support the audit, alongside another provider that was assigned to handle the processing and analysis of Slack data, as that provider had previously created the company’s Slack retention repository. When the Slack portion was delivered, there were noticeable deficiencies in the data set — some of which could have resulted in meaningful problems if an investigation followed the audit.

Because the provider lacked foundational, technical understanding of the nuances of Slack data and their implications in an investigations context, the company ended up spending more and waiting longer for the results. The experts were asked to take over to correct the mistakes and ensure that the Slack data was defensibly preserved and processed, so the organization could respond to auditors confidently.

Global competition authorities and the corporate data universe are moving and evolving swiftly, in parallel. The combined consequences stand to pose new challenges for organizations in preparing for and responding to investigations. Agile, expert-driven approaches, supported by analytics, will be critical in mitigating evolving risks.

Emilia Law

Head of Legal

Novartis

Emilia Law is an experienced head of legal with a demonstrated history of performance in the pharmaceuticals, banking and private equity industries. She is a strong legal professional skilled in mergers & acquisitions, regulatory, data protection, corporate governance, acquisitions, corporate law, and private equity.

Craig Earnshaw

Senior Managing Director

FTI Technology

Craig Earnshaw is a senior managing director within FTI Technology. He provides strategic advice to clients, offering specific counsel to clients on matters involving European Union-based evidence collection and disclosure, regulatory inquiries, computer-based forensics and electronic data hosting for litigation.

Ashley Brickles

Senior Managing Director

FTI Technology

Ashley Brickles is a senior managing director within FTI Technology. She has over 15 years of experience specializing in the use of technology to develop innovative and cost-effective solutions for her clients, and specializes in large, complex multi-jurisdictional regulatory investigations and has led some of the most demanding European cartel and merger-clearance cases over the past decade.