Skadden

White Collar Defense and Investigations

August 26, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

EU Court Upholds Commission's Power To Demand Data Held by Foreign Companies

Summary

In *Nuctech Warsaw* (T-284/24), the EU Court of Justice held that EU subsidiaries can lawfully be required to provide access to email accounts and data held by their overseas parent company. The ruling involved the following framing:

- **Broad reach of EU extraterritorial investigative powers:** The order interprets the European Commission's (EC's) investigative powers broadly. EU law applies to conduct with significant effects in the EU, even if the conduct occurs outside the EU. Consequently, the EC may request information from non-EU companies to assess potential EU law violations.
- **Implications for other EU enforcement regimes:** The investigation was carried out under the EU Foreign Subsidies Regulation (FSR), but the ruling has implications for the EC's powers under general antitrust rules and other regulations such as the Digital Markets Act or the Digital Services Act. The judgment follows divergent rulings in the UK that limited the extraterritorial reach of UK regulators' enforcement powers in fraud and antitrust cases. (See our February 2021 alert "English Supreme Court Limits Serious Fraud Office's Extraterritorial Reach" for more details.)
- **Siloing access to data within a corporate organization:** The ruling held that there was no evidence local subsidiaries could not access China-held data, or that compliance with the EC's inspection decision would compel the applicants and the group to infringe Chinese law, including criminal law. Therefore, companies should consider:
  - If their IT environment and procedures can be siloed to enable the company to demonstrate that accessing parent company data from the EU is not technically feasible without cooperation from the non-EU entities.
  - Whether law and regulation applicable to a company would prevent it from sharing this data with an EU regulator. If so, this should be well-documented in advance, potentially with external legal counsel validation, so that any refusal to comply with a request for data could be quickly substantiated with specific reference to other applicable laws.

Analysis

The EC raided the premises of EU subsidiaries of a Chinese security scanner supplier, Nuctech. The EC requested access to the mailboxes of Chinese employees stored on servers in China. Nuctech's EU subsidiaries challenged the EC's inspection decision (this case is still pending) and, separately, applied for interim measures suspending the inspection decision, together with any subsequent requests by the EC, on the basis that:

- The EC breached public international law by compelling the EU subsidiaries to provide documents stored outside the EU.

EU Court Upholds Commission's Power To Demand Data Held by Foreign Companies

- The EC cannot request documents that are not accessible to the EU entities being inspected.
- Chinese law, including criminal law, prohibited access to such data under threat of fines and periodic penalty payments.

The president of the EU General Court denied this request for interim relief.

He found that there was no breach of public international law in demanding ex-EU-held data because the EC had jurisdiction to demand information and documents stored outside the EU. EU law applies extraterritorially via the qualified effects doctrine, namely where conduct has immediate, substantial and foreseeable effects within the EU. Consequently, the EC may request information from non-EU companies to assess potential EU law violations. Otherwise, the EU would be inviting companies to avoid EU liability by holding data outside the EU.

Further, the court held that the companies had not proven the data was not accessible to them or that Chinese law prohibited access. The court president found that "[t]he applicants have neither explained nor substantiated their claim that they have no access to information stored on servers located in China."

Comment

The case is an interim ruling (and technically *obiter dicta*, since interim relief failed on other grounds), rather than a final judgment. The case may be open to challenge, particularly for reading EU enforcement jurisdiction too broadly given the traditional public international law limits on enforcing investigative measures extraterritorially.

The order leaves open the question of whether local subsidiaries can be compelled to obtain data from a foreign parent company if the data is not technically accessible from the EU. The EC's current practice in antitrust cases during inspections is that the EC is only entitled to data accessible in the ordinary course of business from the local subsidiary.

Meanwhile, the question of extraterritorial investigative powers has been the subject of divergent rulings in the UK, where the Supreme Court held that the Serious Fraud Office (SFO) could not compel overseas documents using domestic powers, but rather should use international mutual assistance treaties.[1] The presumption in that case was that statutes were intended to apply domestically. Conversely, the UK Court of Appeal upheld the Competition & Markets Authority's application of its document production powers extraterritorially to Volkswagen and BMW German parent companies, finding the Competition Act 1998 was a statute with implicit international reach.[2] With similar reasoning to the EU General Court's, the UK Court of Appeal held that to rule otherwise in favour of foreign companies created "a perverse incentive for conspirators to organise cartels directed at harming the UK market."

The UK courts have been consistently skeptical that foreign blocking statutes prevent disclosure in international litigation or enforcement matters. Most recently, the High Court case of *Joshua v. Renault, Stellantis, Peugeot, Citroën and Others* held that, even following a strengthening of the French Blocking Statute in 2022, there remained no real risk of prosecution in France under the statute, and therefore that the applicant could not resist disclosure pursuant to an order of the Court, in favour of a resolution under the Hague Convention.[3] The High Court stated that while it would not lightly make a disclosure order where compliance would entail a party breaching its own criminal law, the Court will, as a matter of comity, assume a respect for English proceedings by foreign courts. The High Court ruling closely followed a similar judgment considering an earlier iteration of the French Blocking Statute by the UK Court of Appeal.[4] Similarly, the EU's order in *Nuctech Warsaw* noted that the company had failed to establish that the production of documents would compel the company to infringe Chinese law, including criminal law, under the threat of fines and periodic penalty payments.

The issue also frequently arises in cross-border matters where U.S. regulatory and enforcement authorities seek to gather evidence located outside of the U.S. Although U.S. authorities generally recognize that non-U.S. laws may apply to limit the production of documents and information located outside of the U.S., companies are still expected to cooperate by producing data within the limits of any applicable laws. For example, the DOJ's Corporate Enforcement and Voluntary Disclosure Policy (updated March 2024) requires "timely voluntary preservation, collection and disclosure of relevant documents and information" for full cooperation credit. The policy states that where a company "claims that disclosure of overseas documents is prohibited or restricted due to data privacy, blocking statutes, or other reasons related to foreign law," then the company bears the burden to show why a non-U.S. law applies and to identify "reasonable and legal alternatives" to help preserve and disclose the necessary documents and evidence. The EU's order in *Nuctech Warsaw*

[1] *R (on the application of KBR, Inc) v. Director of the Serious Fraud Office* [2021] UKSC 2, concerning whether the SFO can require a foreign company to produce documents held overseas, pursuant to its investigation powers under Section 2(3) of the Criminal Justice Act 1987 (CJA).

[2] *CMA v. Volkswagen and Bayerische Motorwerke* [2023] EWCA Civ 1506.

[3] *Joshua & Ors v. Renault SA & Ors (Re Nissan/Renault Diesel NOx Emissions Group Litigation and Peugeot/Citroen/DS NOx Emissions Group Litigation)* [2024] EWHC 1424 (KB).

[4] *Secretary of State for Health and others v. Servier Laboratories Ltd and others* [2019] EWCA Civ 1096.

EU Court Upholds Commission's Power To Demand Data Held by Foreign Companies

likewise specified that the company had failed to explain how Chinese law prevented production and further failed to suggest "other methods which would enable them [company officials] to provide the information without infringing Chinese law."

Takeaways

- Generally, when dealing with requests from regulatory or enforcement authorities to access, preserve or disclose documents and information located in a foreign jurisdiction, companies should conduct a careful analysis of applicable local laws — such as data and information protection and privacy laws, blocking statutes or other applicable national security, data localization or export controls. In both litigation and enforcement proceedings, companies will be better prepared to challenge such requests where they can explain — and provide support for — how local laws prevent them from responding to the requests at issue. Companies should consider documenting this analysis of local laws as preparation to quickly respond to requests from regulators should an investigation begin.
- Companies should consider mapping their data by types, access rights and location, and examine to what extent the sharing of servers and information with, and granting access to, other group entities is appropriate and/or necessary in the normal course of business. Companies should also consider the location of IT support and how that will allow IT teams' full access to the data on the systems they support. Where possible, systems should be designed to restrict access rights by default to local personnel, granting overseas access only where there is a business rationale for doing so. This setup is required by many existing privacy and data localization laws, and is sensible given the *Nuctech Warsaw* decision and other court decisions around the globe.

Contacts

Bill Batchelor
Partner / Brussels
32.2.639.0312
bill.batchelor@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Bora P. Rawcliffe
Counsel / London
44.20.7519.7139
bora.rawcliffe@skadden.com

Ryan D. Junck
Partner / London
44.20.7519.7006
ryan.junck@skadden.com

Nicola Kerr-Shaw
Counsel / London
44.20.7519.7101
nicola.kerr-shaw@skadden.com

Margot Sève
Counsel / Paris
33.1.55.27.11.51
margot.seve@skadden.com

Associates **Aleksandar Leshev** and **Michael D. Traber** contributed to this article.