JONES DAY

COMMENTARY

JANUARY 2018

Retrieval of Mobile Phone Data During Dawn Raids Upheld by Dutch Court

IN SHORT

The Ruling: The far-reaching retrieval of mobile phone data during dawn raids by the Dutch competition authority is permissible, even if encompassing data of a non-business nature, as affirmed by a recent ruling of the Hague District Court.

The Result: Companies cannot challenge such dawn raid seizures of mobile phone data solely on the ground that these also include data of a non-business nature.

Looking Ahead: This court ruling upholds the Netherlands Authority for Consumers and Markets' (the Dutch competition authority) ability to continue to collect and search digital data in line with its current practice, as set out in its 2014 Guidelines on the investigation of digital data.

The Hague District Court confirmed, in summary proceedings in November 2017, that during dawn raids, the Netherlands Authority for Consumers and Markets ("ACM") may make extensive copies of data on mobile phones possibly also containing private data.

The District Court's ruling addressed a request for interim measures following an unannounced on-site inspection of the business premises of an undisclosed company. During the dawn raid, the ACM made digital copies of the data, except for audio recordings, video, and ringtones, on the mobile phones of six employees of the company.

In 2003, the District Court had ruled that the predecessor of the ACM could copy mobile phone data during dawn raids, subject to safeguards to ensure that data of a non-business nature and legally privileged data could subsequently be excluded from the investigation. These safeguards are now enshrined in the ACM's 2014 Guidelines on the investigation of digital data, which set out the handling of digital data collected during investigations of areas of law falling under the ACM's supervision.

> The company indicated that the mobile phones were also used for private purposes and could potentially contain private data. Thus, making digital copies of virtually all data on the mobile phones violated the right to respect for private life.

In contrast with the European Commission's practice, the Guidelines do not provide for on-site inspection of digital data. Instead, digital data is to be secured on-site and subsequently analyzed at the ACM's offices. Before the data collected on-site becomes evidence for the purpose of the investigation, it is filtered in a two-stage process:

- First, an in-scope (i.e., relevant) data set is created by removing out-of-scope data on the basis of specific queries that are first communicated to the party concerned for comments.
- Second, this in-scope data set is made available to the party concerned, who may then request the exclusion of data of a non-business nature, as well as legally privileged data.

The final data set is established once the ACM has assessed the concerned party's requests for exclusion and will include only data that was not subject to an exclusion request and for which such exclusion request was not granted. This data set will be part of the evidence on record and used for the purpose of the investigation.

In the present case, in requesting an injunction to preclude use of the data copied from the mobile phones, the company argued that the aim of the ACM's investigation was not sufficiently clear and that, in any event, the company did not fall within its scope.

Furthermore, the company indicated that the mobile phones were also used for private purposes and could potentially contain private data. Thus, making digital copies of virtually all data on the mobile phones violated the right to respect for private life under the European Convention on Human Rights (Article 8). The company argued that such interference with the right to respect for private life required a prior judicial order and that, in any case, there was no legal basis for copying private data from the mobile phones.

The District Court rejected the request for an injunction for the following reasons:

Due Cause
The District Court held that the ACM had not used its investigatory powers without due cause. It found that the ACM had satisfactorily explained why the company was subject to the investigation and that the investigation's scope was sufficiently detailed and adequate.

Adequate Safeguards
The District Court then examined whether adequate safeguards had precluded the unjustified inspection of data, in line with the judgment in *Vinci v. France* of the European Court of Human Rights ("ECtHR"). The ECtHR held in *Vinci* that, in the case of dawn raids aimed at obtaining evidence of possible anticompetitive practices, the seizure of data must not be widespread and indiscriminate and that the confidentiality of lawyer–client relationships must be respected. To this end, the ECtHR introduced a procedural safeguard, in case the party concerned did not have an opportunity to contest the seizure of data during the dawn raid. This safeguard requires an effective and practical remedy to challenge the validity of the seizure afterward.

In line with a ruling of the District Court in a similar case earlier in 2017, the District Court held that the ACM's Guidelines provided for such procedural safeguard and that there was no legal requirement for a prior judicial order authorizing the seizure of such data.

The District Court further noted with respect to such potential disagreements that, unlike the assessment of requests to exclude legally privileged data, a request concerning data of a non-business nature was assessed by the head of the investigation team instead of an independent official. However, given the possibility of seeking judicial review, the court ruled that the fact that a member of the investigation team would evaluate data to be excluded from the scope of the investigation did not in itself justify an injunction to preclude the ACM from using copies of the challenged mobile phone data.

Additionally, the District Court found that the privacy of the individuals concerned was sufficiently preserved.

Read the Hague District Court's November 22, 2017, judgment.

THREE KEY TAKEAWAYS

1. The increasing digitization of businesses and business communications has shifted antitrust authorities' focus from hard copy to digital data. Due to the nature and volume of digital data, antitrust authorities have developed new practices to collect and search such data.
2. The District Court found that the ACM's practices with respect to dawn raid seizures of digital data, as set out in its Guidelines, provide adequate safeguards to preclude inappropriate access to digital data by the ACM. Thus, parties cannot challenge the seizure of digital data solely on the ground that it might comprise data of a non-business nature.
3. If, subsequent to a dawn raid, a dispute arises concerning data to be used as evidence on the record by the ACM, the concerned parties can seek judicial review of such data use.

CONTACT

Yvan N. Desmedt
Amsterdam / Brussels

Kornel Olsthoorn, an associate in the Amsterdam Office, assisted in the preparation of this Commentary.

YOU MIGHT BE INTERESTED IN: Go To All Recommendations >>

Dutch Court Affirms Ban on Nonauthorized Online Resellers

European General Court Rules (again) on Mandatory Access and Interoperability in Software Industry

Rewarding Loyalty: ECJ Holds that Loyalty Rebates Do Not Per Se Restrict Competition