Kluwer Competition Law Blog

European Commission dawn raids – IT searches

Peter Citron (Editor) (White & Case, Belgium) · Monday, March 25th, 2013

Last week, the European Commission published on its website a revised explanatory note on how it conducts on-the-spot inspections of business premises where it suspects a company has breached competition law (so-called "dawn raids").

During a dawn raid the European Commission has the power to examine and copy not just hard copies of business records, but also electronic information. The most important revisions to the note concern the powers of the inspectors to conduct IT searches.

Extent of IT search
The revised note provides the following non-exhaustive examples of the IT storage media that the inspectors may search during an inspection: laptops, desktops, tablets, mobile phones, CD-ROMs, DVDs, and USB-keys.

The guidelines note that storage media that is examined will be kept by the inspectors until the end of the inspection, but *"may be returned earlier, for instance after a forensic copy of the data under investigation has been made"*.

Business executives should therefore be prepared that they may have to hand over to the inspectors their blackberry and/or smartphone during an inspection. They may be requested for passwords for these items and a forensic copy of the data on these devices may be made. They should be prepared to manage their work schedule without these devices for several hours, and at worst until the end of the raid (which may last as long as three days).

Forensic IT tools
The revised note emphasises that the inspectors may not only use built-in keyword search tools for their IT searches, but also their own dedicated software and/or hardware. These tools allow the inspectors to copy, search, and recover data *"whilst respecting the integrity of the undertakings' systems and data"*. In practice the inspectors may image data from the company's hard drive and place a copy on a PC brought by the inspectors. They will then run searches on the copy data using their own forensic software.

The note states that at the end of the inspection the inspectors cleanse all the forensic IT tools that contain data from the undertaking. The goal is to completely remove the company's data from the PC brought by the inspectors *"in a way that the data cannot be reconstructed by any known technique"*. Hardware provided by the undertaking will not be cleansed by the inspectors.

Assistance from the company

The revised note states that an undertaking may be required to provide staff to assist the inspectors *"not only for explanations on the organisation of the undertaking and its IT environment, but also for specific tasks such as the temporary blocking of individual email accounts, temporarily disconnecting running computers from the network, removing and re-installing hard drives from computers and providing "administrator access rights'- support". When such actions are taken, the undertaking must not interfere in any way with these measures and it is the undertaking's responsibility to inform the employees affected accordingly. The Inspectors may ask to use hardware (hard disk, CD-ROM, DVD, USB-key, connection cables, scanner, printer and so) provided by the undertaking but cannot be obliged to use the undertaking's hardware."*

This requirement underlines the importance of companies training their IT staff as well as their general staff on dawn raid defence best practice, as they may be directly involved in a dawn raid. Inappropriate behaviour by IT and other staff can be costly.

On 28 March 2012, the European Commission imposed fines of €2.5m on two Czech power companies for obstruction in relation to electronic documents. During the raid the European Commission requested access to email accounts to be blocked by setting a password known only to the European Commission (to prevent tampering with emails during the raid). However, the password for one email account was modified by the company to allow the relevant employee to access the account. In addition, during the course of the raid an employee requested the IT department to divert all incoming emails to certain blocked email accounts to a server, which prevented the European Commission obtaining access to these emails for review.

Continuation of the raid at the European Commission's premises

The revised note retains (whilst slightly amending the wording) a paragraph which emphasises that the European Commission has a right to effectively continue its review at the European Commission's premises. The procedure is described as follows: *"If the selection of the relevant documents for the investigation is not finished during the inspection on the undertaking's premises, the copy of the data still to be searched is secured by placing it in a sealed envelope and the undertaking will be provided with a duplicate. The Commission commits to return the sealed envelope to the undertaking or to invite the undertaking to attend the opening of the sealed envelope at the Commission premises and assist in the continued selection process".*

This specific practice was challenged in the recent Nexans case before the General Court (Case T-135/09), where Nexans argued that the European Commission had no power under the relevant legislation to take away the forensic copies of computer hard drives for later review at the European Commission's premises, as its powers were limited to searching for relevant documents on a company's site. The General Court, however, did not rule on the legality of this practice as it found that this challenge was inadmissible. It can be expected that the power of the European Commission to continue forensic searches at the Commission's premises after a raid, even in the presence of the company, will be challenged in other cases before the Court of Justice of the European Union.

Conclusion – a training need

It is essential that companies train their staff on how to deal with dawn raids effectively. The European Commission's enhanced focus on IT search means that companies must also include IT staff in this training.

To make sure you do not miss out on regular updates from the Kluwer Competition Law Blog, please subscribe here.

This entry was posted on Monday, March 25th, 2013 at 4:50 pm and is filed under Source: OECD“>Antitrust, Source: OECD“>Competition, Source: UNCTAD

“>Dominance, European Commission
You can follow any responses to this entry through the Comments (RSS) feed. You can skip to the end and leave a response. Pinging is currently not allowed.