Kluwer Competition Law Blog

Personal electronic data in competition investigations: The inequality of arms between companies and the Commission

Jessica Walch (Sidley Austin LLP) · Thursday, November 8th, 2012

In the context of antitrust and cartel investigations, electronic data or computer-generated information often has the highest evidential value and potentially the highest impact on the outcome of the investigation. For this reason, when conducting surprise inspections at the premises of a suspected undertaking, electronic data is often the first target of the Commission.

Companies may already be well versed in the usual notes of caution. For examples, it is highly recommended that an external counsel be present to supervise Commission officials' access to electronic data. In the event that materials are legally privileged, the company has the right to object to the Commission's taking the document and escalate any potential dispute before the Hearing Officer.

An area that is less often considered however relates to the potential seizure of personal data. In the event that the information in the documents searched by the Commission constitutes personal data, the undertaking is under the obligation to cooperate with the Commission and protection of personal data will not be a valid basis on which to refuse access. This gives rise to a potential inequality of arms between the Commission and the company under investigation because, under existing legislation, the Commission has greater rights of access to those data than the company itself.

Legal standards allowing for the processing of personal data

Directive 95/46/EC on personal data protection (the "Directive") currently requires companies to obtain consent before processing personal data unless they have a legitimate purpose for doing so.[1] However, the Directive does not apply to the Commission which is, instead, subject to Regulation EC/45/2001, which contains less restrictive rules regarding access to citizens' personal data.[2]

The Commission has recently proposed a comprehensive reform of EU data protection rules with the objective of introducing (i) a single set of rules on data protection, applicable to all companies across the EU[3] and (ii) a new directive that will apply general data protection principles in the context of police and judicial cooperation in criminal matters.[4] As part of the discussions during the legislative process, the lead parliamentary committee has recently said that there could be an agreement amongst Members of the European Parliament to extend the scope of the new

Regulation to cover EU institutions.[5]

In the context of surprise inspections, the Commission, as an investigator, would normally have a legitimate purpose to process personal data and may access certain employees' personal electronic communications. It seems logical that once the Commission has seized an employee's personal data, the company will have a legitimate purpose for looking at it too.

However, the point of seizure by the Commission may be the first time that company has the right to know what is in its own records. When undertakings conduct internal investigations to assess their own compliance with EU competition rules or with the objective of applying for immunity or reduction of a fine, they will have to obtain voluntary and specific consent from each of the employee(s) concerned before they can even establish whether relevant information and evidence exists within the personal data held.

Companies' internal rules may further restrict access to employees' emails by requiring for example the presence of the employee for the employer to access his/her work-related or personal emails.[6] Therefore, attention must be paid to companies' internal policies before initiating an internal investigation.

There can be some exceptions to the obligation upon companies to get specific consent, for example if a company can justify that it has a legitimate purpose for processing such data (e.g. suspected perpetration of criminal offences by the employee). However, before the opening of any administrative procedure by the Commission or other regulator, it may be difficult for a company to demonstrate its legitimate purpose for accessing its employees' personal data, should they refuse to give consent.

Conclusion

In practice, when examining data during the dawn-raid, the Commission will rely on the scope of its investigation to assess the relevance of the documents to be seized, including personal electronic data falling within this scope. It might also try to seize a copy of a server or other storage medium that can potentially include personal information, in the hope of conducting its searches at the Commission's premises, under the supervision of the undertaking.[7]

Given the far-reaching nature of the Commission's enforcement powers during surprise inspections as regards personal electronic communications, companies must understand that the Commission may have more unrestricted access to internal records than even the company itself has had until that point.

In building a compliance structure it is therefore important for companies to consider the extent to which they are allowed to monitor employees' email traffic, and be as transparent as possible during this process in accordance with national data protection rules. It is also worth establishing the basis for a consent request in each employees contract and in internal policies at the outset so that it is clear that consent may be requested for internal housekeeping and compliance exercises (bearing in mind that, should the employees' consent be necessary, it has to be voluntary and specific).

At a policy level the inequality of arms gives rise to serious rights of defence issues. At present the Commission can use personal data against a company even though that company had no means to

know about it, to access it or to control it prior to its seizure. While this inequality of arms might be addressed in the upcoming legislative review, at present companies must simply be vigilant and be aware that they start from a disadvantage when fighting the compliance battle.

The opinions expressed herein are those of the authors and do not necessarily reflect the views of their respective firms, clients, or any affiliates of any of the foregoing. This article has been prepared for informational purposes only and does not constitute legal advice.

References[+]

This entry was posted on Thursday, November 8th, 2012 at 12:11 pm and is filed under Source: OECD“>Competition
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.