CLEARY GOTTLIEB

Digital evidence gathering in dawn raids – the company's perspective

Dr. Romina Polley, Partner, Cleary Gottlieb Steen & Hamilton LLP

20th St. Gallen International Competition Law Forum ICF, April 4, 2013

Introduction

- In an increasingly paperless world, focus shifts to digital evidence gathering
- Volume of electronic data is ever increasing
- IT systems get more and more complex, e.g. cloud computing
- Search tools become more sophisticated
- Sifting through millions of e-mails is very costly

Digital evidence gathering is a challenge for the Commission

- Dependence on company's cooperation, *e.g*. get explanations on IT infrastructure and access to passwords, technical assistance by IT staff
- Difficulty to find “smoking gun” pieces in huge electronic files during on-site review
- Risk of being accused of fishing expeditions if search terms are not precise enough
- Strain on resources if inspections last very long

Digital evidence gathering is a walk on a tightrope for the company concerned

- Failure to cooperate during inspection or obstruction of digital evidence gathering by inspectors may lead to separate fines (Article 23 (1) c Regulation 1/2003; see for example Commission decision of March 28, 2012 in Case COMP/39793 – *EPH and others*) or an increased fine for the infringement

- Cooperation on IT issues can be tricky in practice, *e.g*. administrator access rights support

- Legitimate interest in exercising rights of defence and protecting confidential data

- Absence of effective judicial review aggravates the situation

The Commission’s approach to digital evidence gathering

- Inspectors are empowered "to examine the books and other records related to the business, irrespective of the medium on which they are stored" (Article 20 (2) b Regulation 1/2003)

- Commission Explanatory Note of 2013, paras 9-14
  - Full image of server or storage media for safekeeping purposes (forensic copy) and blocking of individual email accounts
  - Preview of storage media, *e.g*. laptop, with EnCase software
  - Storage media indexed to allow for keyword searches with built-in search tool or forensic IT tool
  - Commission claims access to all information accessible on-site irrespective of server location
  - Print outs of results of keyword searches are made and added to document list
  - Sealed envelope procedure also referred to as “mirroring” where electronic data is carried away *en masse* from company's premises so far only used in exceptional cases

Legal Concerns (1)

- Access to electronic data located outside the European Union goes beyond the European Commission's investigation powers,
  - Within the EU assistance of NCA is a possibility,
  - Outside the EU cooperation with competition authorities on the basis of cooperation treaties only
  - „*Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system*“ (Art. 19 (2) of Convention on Cybercrime)

- Trans-border access to stored computer data only with consent of the state where data is stored or in case of publicly available data (Art. 32 of Convention on Cybercrime)

- Inspection decision does not cover third party service providers

Legal Concerns (2)

- Protection of documents outside the scope of the investigation:
  - “Information exchange shall only be used in respect of the subject matter for which it was collected by the transmitting authority" (Article 12 (2) Regulation 1/2003)

- Search for digital evidence should not be tantamount to a fishing expedition
  - Commission is required to specify the subject matter of the investigation (*Hoechst*, Judgment of the Court of September 21, 1989*,* paras 40-41; *Dow Benelux*, Judgment of the Court of October 17, 1989, paras 7-8)
  - Commission must identify the sectors covered by the alleged infringement with which the investigation is concerned with a degree of precision sufficient to enable the undertaking in question to limit its cooperation to its activities in the sectors in respect of which the Commission has reasonable grounds for suspecting an infringement of the competition rules, justifying interference in the undertaking’s sphere of private activity (*Nexans*, Judgment of the General Court of November 14, 2012, para. 45)

- Relationship between documents requested and the alleged infringement required, they should help to determine whether the infringement has taken place (*SEP*, Judgment of the General Court of December 12, 1991, para.25)

Legal Concerns (3)

- Company does not get access to search terms and cannot influence them!

- No protection against self-incrimination applies to documents copied during inspections (*Orkem*, Judgment of the Court of October 18, 1989, para. 34; *SGL Carbon*, Judgment of the Court of June 29, 2006, para. 41), but: ECtHR applies privilege to pre-existing documents in certain situations (*Funke/France*, Judgment of the ECtHR of February 25, 1993, para. 44; *JB/Switzerland*, Judgment of the ECtHR of May 3, 2001, paras 64 and 71)

- According to ECtHR the right to privacy (Article 8 ECHR) encompasses the privacy of business premises (*Niemietz,* Judgment of the ECtHR of December 16, 1992, para. 30; *Colas Est,* Judgment of the ECtHR of April 16, 2002, para. 41), acknowledged by ECJ in *Roquette Frères* (Judgment of the Court of October 22, 2002, para. 29), but exception in Article 8 (2) "right of interference of the investigating authorities may be more generous where business premises are concerned", to be revisited after Lisbon Treaty (Article 7 CFREU)?

Legal Concerns (4)

- Legal professional privilege should be respected
  - Confidentiality of communication between independent outside counsel and client form part of the rights of defence (*AM&S*, Judgment of the Court of May 18, 1982, paras 18 *et seq.*)
  - Commission cannot even take a cursory look at those documents (*Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd*, Judgment of the General Court of September 17, 2007, para. 82)

- Protection of Business Secrets (Article 30 (2) Regulation 1/2003)

- Protection of private documents
  - Documents of non-business nature are outside the scope of the investigation (*Roquette Frères,* Judgment of the Court of October 22, 2002, para. 45)

- Data protection rules not respected by Commission in information gathering whereas company under obligation to respect data protection rules in internal investigations

- Broad scope of mirroring and potential for abuse would require effective judicial review

Judicial review by the EU Courts (1)

- Limited but gradually increasing judicial review over inspection decisions
  - Lack of evidence, reasoning or non-compliance with proportionality principle (*Dow Chemical Iberica*, Judgment of the Court of October 17, 1989, paras 45-53)
  - Reasonable factual grounds for suspecting an infringement (*Roquette Frères*, Judgment of the Court of October 22, 2002, para. 54)
  - Sector concerned needs to be identified with precision (*Nexans*, Judgment of the General Court of November 14, 2012, para. 45)
- However, disputes over procedural issues occurring during the inspections cannot be challenged in advance of a final infringement decision unless they produce binding legal effects (*Nexans*, Judgment of the General Court of November 14, 2012, para. 115)
- Immediate judicial review only acknowledged for inspection decisions (see *Dow Benelux* and *Roquette Frères*) and privileged documents (*AM &S*, Judgment of the Court of May 18, 1982, para. 32; *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd*, Judgment of the General Court of September 17, 2007, para. 45)

Judicial review by the EU Courts (2)

- Mirroring pure implementing measure and therefore no reviewable act in its own right (*Nexans,* Judgment of the General Court of November 14, 2012, para. 132)

- Alternative of provoking a Commission decision fining the company for obstruction by refusing to submit to the mirroring exercise (Article 23 (1) Reg. 1/2003)?
  - EU law principle that you should not be forced to violate a rule in order to get a legal remedy (*Unibet*, Judgment of the Court of March 13, 2007, para.64)
  - Opportunity may not arise if Commission decides not impose separate fine but to increase fine for infringement only (aggravating circumstance)

- Judicial review through challenging of the final fining decision can be extremely belated - from a dawn raid until the final fining decision more than 3.5 years in average go by

- Action for non-contractual liability of measures that cause investigated party to suffer harm

- Does the actual state of judicial review in case of mirroring really meet the requirements from the fundamental right to an effective remedy enshrined in Article 47 (1) CFREU?

Tension with Strasbourg case-law on legality of inspections and digital evidence gathering (1)

- Requirements developed in the *Ravon* (Judgment of the ECtHR of February 21, 2008, para. 28), *Primagaz* (Judgment of the ECtHR of December 21, 2010, para. 28), *Canal Plus* (Judgment of the ECtHR of December 21, 2010, paras 36 and 44) and *Robathin* (Judgment of the ECtHR of July 3, 2012, para. 52) judgments:

  - Possibility of review of the inspection decision both on facts and on points of law
  - A court should be able to assess necessity and proportionality of the inspection
  - Domestic law and practice must afford adequate and effective safeguards against abuse and arbitrariness
  - The appeal should, if it is well founded, either prevent the enforcement of the inspection decision or provide for an effective remedy
  - Effective remedy means also the certainty of effective judicial review within a reasonable time
  - Deficiencies in the limitation of the scope of the search warrant can be offset by sufficient procedural safeguards

Tension with Strasbourg case-law on legality of inspections and digital evidence gathering (2)

- Search of all electronic data (as in mirroring) should be justified by particular reasons and be proportionate to the circumstances of the case (*Robathin*, paras 50-52)

- See also *Schenker/EFTA Surveillance Authority* (Judgment of the EFTA Court of December 21, 2012) referring to *Robathin* standard in third party access to documents in competition case setting

- Through Art. 52 (3) CFREU the ECtHR case law becomes indirectly binding for the EU institutions

- Tension between Strasbourg and Luxembourg case law:
  - The ECtHR case law seems to require possibility of examination of necessity and proportionality of mirroring on a stand-alone basis, while the GC seems to consider an incidental assessment within the appeal against a final fining decision as sufficient protection of fundamental rights

  - Currently no safeguards available in case that search terms plainly fall outside the scope of a valid inspection decision – problematic review of proportionality!

The national perspective – digital evidence gathering by the FCO

- FCO also follows the „access approach“ claiming right to get copies of any data the company has access to irrespective of server location
- Company under no duty to active cooperation, but inspectors can hear witnesses on IT infrastructure and passwords
- Contrary to the Commission, the FCO can seize IT-hardware
- Unlike the Commission, the FCO usually collects electronic data *en masse* during the inspection and searches for evidence with the use of IT forensics later at its own premises
- FCO does not allow lawyers or representatives of the company to attend sifting of electronic data at its own premises
- After the end of the review of the IT files, the FCO sends to the inspected company a DVD containing the evidence found and a list of the used search terms

Conclusion

- Mirroring can be necessary to ensure effective enforcement of competition law, but there have to be specific reasons to allow for the off-site search of data outside the scope of the infringement
- Necessity and proportionality test should be applied having regard to the specfic circumstances
- Effective judicial review is needed to avoid abuse and arbitrariness
- Only stand-alone appeal against mirroring would provide the necessary procedural safeguards, because review of final infringement decision comes too late

NEW YORK

WASHINGTON

PARIS

BRUSSELS

LONDON

MOSCOW

FRANKFURT

COLOGNE

ROME

MILAN

HONG KONG

BEIJING

BUENOS AIRES

SÃO PAULO

ABU DHABI

SEOUL

CLEARY GOTTLIEB STEEN & HAMILTON LLP

www.clearygottlieb.com