

New Issues in Cartel Enforcement

Marc Hansen
Niall Lynch
Daiske Yoshida

Tokyo - Fair Trade Center - 9 November 2011

LATHAM & WATKINS

2011 – A year of active enforcement

- Very large cases – E.g., automotive industry investigations
- Increasing global coordination
- Realisation that parallel investigations by authorities around the world creates problems
- Authorities increasingly focused on not obstructing each others' cases (coordination and alignment of enforcement)
- Several authorities reviewing their leniency programs to ensure incentives remain attractive for leniency applicants

Issues of 2011

- What is a “hardcore conduct” – information exchanges in EU
- Significant increase in use of US “amnesty plus”
 - Led to many new investigations (automotive industry)
 - Knock-on effect on other countries / Needed outside US?
- Standards for immunity markers and perfection of markers
- What is the duty of cooperation by a leniency applicant
 - Admissions / Documents from other jurisdictions / Translation costs
- Cross-border evidence collection issues
 - “Cloud” based computing / where is server located?
- Civil litigation disclosure risks from leniency admissions
 - Pfleiderer / US discovery litigation
- Waiver of privilege
 - UK OFT Review / ACCC new criminal regime

The Automotive Cases

- The automotive industry investigation is the largest ever for DOJ and EU, and for many other authorities
- Why this industry?
 - Procurement patterns by automotive companies
 - Barriers to entry for suppliers
 - Collaborative development/cost concerns in R&D phase
 - Competitive RFQs, but few qualified bidders
 - Annual cost reduction targets and negotiations
 - Qualified suppliers under pressure to bid
- How have the investigations developed...

The evolution of the Automotive Cases

- The automotive industry investigation shows the efficacy of the leniency systems across the globe
- Immunity and amnesty applications
 - Supplier 1 of Product A
- Amnesty Plus application in US
 - Supplier 2 makes Products A and B
- Global coordination by authorities and leniency applicants
 - Cases spread across US, EU, UK, Japan
- News reports (MLEX) indicate broad scope and several cases:
 - Wire harness and electrical components
 - Safety equipment (seatbelts; airbags etc)
 - Alternators, starters, ignition parts and electronics
 - Automotive electronics and electrical systems

What lessons can be learnt?

- Cases can spread widely and quickly
- Companies involved in an investigation need to get a full overview of their exposure
- When cooperating with the authorities
 - Cooperate everywhere
 - Cooperate and disclose fully
 - If not, risk of “tag-back” (i.e., being caught by later cases)
- Customers should review procurement processes
 - Work with suppliers to minimize risk of collusion
 - Separate commercial and technical functions
- Beware of information exchanges – Creates liability in EU

EU Cartel Enforcement: Current Issues in Evidence Gathering

Marc Hansen

Tokyo, 9 November 2011

LATHAM & WATKINS

Evidence Gathering and Obstruction

- Why evidence gathering as the topic of the day?
- A focal point of many recent “non-cooperation” cases:
 - Dawn raids (unannounced inspections)
 - Gathering of electronic evidence in the EU
 - Access to evidence located outside the EU
 - Personal email accounts and telephone records
 - Enforcement trends: stricter attitude toward obstruction
- Rules when a company is cooperating/leniency applicant

Dawn Raids

- Only at locations inside EEA/EU; Cannot refuse access
- Lawyers can be present, but EU will not wait long
- Inspection decision defines scope of search
- Seize hardcopy documents within scope
 - Private diaries / fundamental rights EHCR
- EU position: Seize data on EU-based PCs is accessible in ordinary course of business, irrespective of server location

Evidence Gathering - Forensic IT

- Since 2008, forensic IT training of Commission officials
- Commission explanatory note on inspection decisions: power to take "*integral copy of digital storage medium*"
- Use of in-built search facility of devices searched and dedicated software/hardware brought in by the Commission
- Preview of data with ENCASE software, allowing recovery of digital evidence in deleted files and reformatted disks
- Selection of relevant documents made on the spot, if possible
- Otherwise, copy in sealed envelope / searched at Commission premises with counsel's presence to ensure protection of legal privilege and privacy.

Forensic IT – Case Study: Power Cables

- *Power Cables* cartel, Commission takes full image of laptops of executives
- Huge amount of data seized: thousands of pages, years of emails
- Forensic software allows recovery of deleted data
- Defeating encryption
- PC “forensic” image put in sealed envelope, reviewed one month after at Commission premises with companies' counsel
- Companies appeal inspection decision to EU General Court:
 - Right to inspect company's record is limited to company premises.
 - No wholesale copy of data
 - Wholesale copy may result in seizing privileged/private documents
 - Risk of "fishing expeditions"
 - Hearing in October 2011. Ruling expected in 2012

Access to evidence located outside the EU

- Hot issue in international cartel enforcement
- No case law. Need for careful scrutiny of EU practice
- Three different scenarios. Commission may be seeking:
 - Information located outside the EU - from non-EU entity
 - Information located outside the EU - from EU entity
 - Information on server outside the EU - accessible by EU entity

Request for information to non-EU company

- Can the Commission request information located outside the EU from non-EU entity (e.g. Japanese parent company)?
- The law is unclear; In principle, such a request is not possible:
 - Commission lacks jurisdiction
 - Territoriality, sovereignty, comity, non-intervention in foreign States
 - EU cannot, as the US, use MLAT to get documents in Japan
- However, note :
 - Commission practice is to send request to non-EU entity (no duty to reply...but may negatively affect EU view of whether company is cooperating)
 - Commission official position is not to send binding requests to non-EU entity (.. but it has not excluded doing so)
 - If Leniency Applicant, all information must be provided

Request non-EU information sent to EU Subsidiary

- Can the Commission request information located outside the EU from EU subsidiary (e.g. information located at Japanese HQ)?
- Commission may impose fine up to 1% of total revenue if answer not provided in time and periodic penalty for each day of delay
 - *Microsoft Penalty Payment* (€ 899 million fine!); *Baccarat*
 - Recent precedents by NCA (Austria, Germany, Luxembourg)
- Most companies comply voluntarily
 - Do they have to? Leniency and other cooperation
- *Chi Mei*: EU sub of Taiwanese parent company got binding RFI:
 - EU subs only active in repair and marketing, no production or sales
 - RFI sought information under the control of Taiwanese parent
 - EU subs file appeal against RFI, challenging legal basis
 - Action withdrawn following management change; no judgment

EU position on RFIs to subsidiary for information located outside the EU and under control of parent

- Commission position: location of information is irrelevant if:
 - Subsidiaries part of same "*undertaking*" as parent
 - Commission reasonably expects subsidiaries can access information
- However:
 - Reg. 1/2003 gives Commission powers to request information from locations "*throughout the Community*"
 - "*Economic unit*" theory upside down: subsidiary liable for parent
- EU considers it can address request to any part of the *Undertaking*
- But,
 - Acts of EU institution cannot create rights / obligations outside EU
 - Art. 211 TFEU – “the Union [...] shall cooperate with third countries”

Accessing a non-EU Server from inside the EU

- Can the Commission access information located on non-EU Server which is electronically accessible from EU (e.g. mail server or Accounting data)?
 - Commission current position: Yes
 - Article 20 Reg. 1/2003: right "*to examine the books and other records related to the business, irrespective of the medium on which they are stored*"
 - Access to IT server regardless of location if accessible to personnel in ordinary course of business
 - Commission may request warrant to access from another company location in the EU where data available on ordinary course of business
 - Important to design data access rights and policies

Collecting Private Information

- European Commission access to private email accounts
 - EU regularly requests access, irrespective of information being located on private account
 - EU Data Privacy concerns, position of national privacy authorities
 - In a recent case, Commission requested (and obtained) emails stored in private accounts that employees used for professional purposes
- Telephone records
 - Will European telephone service operators grant the company access to detailed telephone records required to respond to EU RFI?
 - What can the EU do?
 - What is duty of a leniency applicant?

EU Enforcement: Obstruction

Stricter treatment of obstruction – watch your IT department !

- In the past, obstruction led to increase in fine
 - Professional Video Tapes (Sony - aggravating circumstance)
- Obstruction now separately investigated; Fine < 1% of revenues!
 - Commission Decision of January 2008 against E.On.: fine of € 51 million for breaking seals affixed in premises undergoing inspection
 - In May 2010, Commission opened investigation against Czech J&T and EP Holding, alleging "*a number of incidents relating to the handling of e-mail accounts and the access to electronic records occurred*"
- Conclusions:
 - Be aware of powers of Commission and growing IT capabilities
 - Ensure training of personnel re data retention and inspections
 - Legal issues: how far can the Commission go?

Discovery of Foreign Located Documents: The Limits of International Discovery

Niall E. Lynch
Tokyo, 9 November 2011

LATHAM & WATKINS

Grand Jury Subpoenas and Search Warrants – Primary Tools For Gathering Evidence in U.S.

- **Corporate Subpoenas**
 - Documents (*duces tecum*)
 - No Fifth Amendment right to refuse to produce
 - Broadly drafted to capture extensive number of documents
 - Calendars, notebooks, diaries, emails, phone records, memorandum, travel and expense records, financial records
- **Individual Subpoenas**
 - Documents (*duces tecum*)
 - Testimony (*ad testificandum*)
 - Implicates Fifth Amendment right against self-incrimination
 - Usually requires grant of immunity before witness will testify
- **Search Warrants**

Geographic Limits of Grand Jury Subpoenas and Search Warrants

- As a matter of prosecutorial discretion and international comity grand jury subpoenas and search warrants only require production of documents located within the U.S.
 - Some case law supports power of grand jury to compel production of foreign located documents, usually bank records. See U.S. v. First National Bank, 396 F.2d 897, 900 (2nd Cir. 1968); Matter of Marc Rich & Co. AG, 707 F.2d 663, 668 (2nd Cir. 1983)
 - But DOJ does not enforce this right: “*Division’s normal procedure is to accompany subpoenas . . . with a note to the effect that production of foreign materials should be considered voluntary . . .*” Handbook on Antitrust Grand Jury Investigations (ABA, Section of Antitrust Law 3d ed. 2002) at 293.
- Example: Foreign Located Electronic Documents Accessible from Computers in the U.S.

Sources of Foreign Based Documents for DOJ

- **Leniency Applicants**

- *“providing promptly, and without requirement of subpoena, all documents, information, or other materials in its possession, custody, or control, **wherever located**, not privileged under the attorney-client privilege or work-product privilege, requested by the Antitrust Division . . .”* Model Leniency Letter

- **Cooperating Defendants**

- *“producing to the United States all non-privileged documents, information, and other materials, **wherever located**, in the possession, custody, or control of the defendant or any of its related entities, requested by the United States . . .”* Model Plea Agreement

- **MLATs or Letters Rogatory**

- Applies to both documents and testimony from witnesses
- Can be difficult and time consuming.
- Has recently been successfully used by DOJ. *See In re Air Cargo Shipping Services Antitrust Litigation, 2010 WL 1189341 (E.D.N.Y.)*

New Source of Foreign Located Documents for DOJ: Civil Discovery

- In follow-on civil litigation in the U.S. the plaintiffs can, and regularly do, require defendants to produce foreign located documents.
- Once the documents are brought into the U.S. the DOJ can issue a grand jury subpoena to the companies or law firms for the documents.
 - *See In re: Grand Jury Subpoenas served on White & Case et al.*, 627 F.3d 1143 (9th Cir. 2010) (Holding that a grand jury can subpoena foreign based documents subject to civil protective order.) Cf. *Martindell v. Int'l Tel. & Tel. Corp.*, 594 F.2d 291, 295 (2d Cir. 1979) (grand jury subpoena will only trump a protective order where “improvidence in the grant of a . . . protective order,” “compelling need,” or “extraordinary circumstance.”)

How to Effectively Handle Document Review in Cartel Investigations

- Instruct client to preserve all responsive documents
- Keep documents in original location (don't move them around the globe)
- Conduct document review outside the U.S.
- Insist that Joint Defense Agreements contain provisions limiting transfer of documents (for companies and individuals)
- Seek stay of civil discovery pending completion of grand jury investigation
- Resist production in the civil case and consider consequences of civil contempt order or adverse inference in civil proceedings, especially if there is an opportunity to cure the refusal to produce (cost/benefit analysis)
- Produce foreign-located documents to civil plaintiffs abroad
- Ultimately, you may be able to delay, but not prevent, the documents from ending up in the hands of the DOJ

New Twist in U.S. Civil Discovery: Targeting the EC & JFTC Investigations

- Requests for Written Submissions to the EC
 - In re Vitamins Antitrust Litig., 120 F. Supp. 2d 58 (D.D.C. 2000)(required production of written submissions to EC)
 - In re Methionine Antitrust Litig., No. C99-3491 (N.D. Cal. June 17, 2002)(did not require production of written submissions to EC)
- Copies of the SO and Oral Hearing Transcript
 - In re Payment Card Interchange Fee and Merchant Discount Antitrust Litig., 05-MD-2010 U.S. Dist. LEXIS 89275 (E.D. N.Y. Aug. 27, 2010)(motion to compel denied)
- All communications and documents exchanged with EC & JFTC
 - In re TFT-LCD (Flat Panel) Antitrust Litig., 07-MD-1827 Doc. No. 2686 (N.D. Cal. April 26, 2011)(after *in camera* review motion to compel denied)
- Final Unredacted EC Decision
 - In re Air Cargo Shipping Services Antitrust Litig., MDL No. 1775 (motion to compel pending)

Contact Information

- **Marc Hansen**
Latham & Watkins
99 Bishopsgate
London, EC2M 3XF

Latham & Watkins LLP
44 Boulevard du Regent
1000 Brussels, Belgium

Tel: +44 20 7710 1094
E-mail: marc.hansen@lw.com
- **Niall E. Lynch**
Latham & Watkins LLP
505 Montgomery Street
San Francisco, CA 94111-6538

Tel: +1.415.395.8162
E-mail: niall.lynch@lw.com
- **Daiske Yoshida**
Latham & Watkins Gaikokuho Joint Enterprise
Marounichi Building, 32nd Floor
2-4-1 Marunouchi, Chiyoda-ku
Tokyo 100-6332

Tel: +81.3.6212.7800
E-mail: daiske.yoshida@lw.com