

Managing Electronic Information:

Legal Risks Involving the U.S., EC, Hackers and Leakers

8 February 2011

**Flip Petillion
Thomas De Meese
Jeane Thomas**

Tuesday, 8 February 2011

Agenda

1. **Belgian Perspective**
2. **Electronic Data in Antitrust Investigations**
3. **e-Discovery in the U.S.**

Belgian perspective

- Internal information management
- External information management
- Special regulation regarding e-information
- Special regulation regarding telecom companies

Internal information management

- Art. 17 « WAO »

- Contractual clauses
 - Confidentiality
 - IP and non-IP
 - Training
 - Non-competition
 - Non-solicitation
 - Non-application

Internal information management

- « CAO » n° 81 – Personal Data Protection Law of 8.12.1992 :
 - to protect employees' privacy against the control of the electronic online communication data

- « CAO » n° 81: 3 essential principles:
 1. Finality: collecting and processing for individualization – permitted in a limited number of cases:
 - 1° prevention of unauthorized and defamatory facts, facts that are contrary to morality or could harm another person's dignity;
 - 2° protection of confidential economic, commercial and financial interests of the company and fight against practices that are conflicting with these interests;
 - 3° safety and / or proper technical functioning of the IT network systems of the company, including supervision of the costs involved and physical protection of the company's facilities;
 - 4° compliance in good faith with the principles and rules applicable within the company for the use of online technology.

Internal information management

Example # 1:

- Hacking of computers, among which
 - Unlawfully taking note of electronic online communication data on staff management or confidential medical files
 - Consulting pornographic or pedophile sites and sites that incite to discrimination, segregation, hate or violence against a group, community or its members, because of race, color, religion or national or ethnic origin of these members or of some among them
- Illustration: Labour Court of Appeal Ghent, 4 April 2001:
 - IT abuse: sending an e-mail on behalf of a third person without permission and using the ICT manager's mailbox

Internal information management

Example # 2:

- Disparaging advertising as stipulated in “WMC”
- Circulation of files and violation of business secrets, including research and development, production processes and all other possible confidential data
- Cf.: Art. 17. “WAO”:
 - Legal basis for control? Minority: Yes!

Internal information management

2. Proportionality: control must be adequate, relevant and not excessive - no unnecessary interference into privacy
 - control of the websites: collection of data on the duration of the connection per workstation and no individualization of the consulted websites
 - control of the use of electronic mail: collection of data on the number of outgoing messages per workstation and the volume thereof and no identification of the employee who sends them

3. Transparency: informing and consulting employees
 - Individualization without formalities in serious cases:
 - wrongful facts
 - protection of the interests of the company
 - protection of the network of the company

 - Alarm proceedings:
 - Informing of an irregularity
 - Informing of a future individualization - in case of repeated irregularity

Internal information management

- Sanction:
 - Supreme Court 2003, 2005 and 2008:
 - Illegal evidence can be used, except:
 - Formalities prescribed under penalty of nullity
 - Unlawfulness affects the evidence's reliability
 - Use of evidence is contrary to fair trial
 - Criminal cases
 - Also for employment agreements?
 - In practice:
 - No uniform case law
 - But: Court of Ghent 1 September 2008
 - CAO n° 81: not under penalty of nullity
 - Evidence is reliable
 - Employee had fair trial

Internal information management

- Actions

- President of the Labour Court

- Cease and desist
- Ex-employee – new employer
- Writ of summons (urgency!) or ex parte request (absolute necessity)

- President of the Court of first instance

- Counterfeit seizure

External information management

- Replying to requests
 - In the context of proceedings
 - On an authority's request
- In the context of proceedings: Evidence conservation
 - Not of public order or imperative law
 - Exception: **WMPC**, art. 74, 21° consumer protection

External information management

- Production of evidence / on an authority's request
 - Conservation in view of prescription periods
 - Conservation in view of mandatory cooperation in the production of evidence
 - *Art. 871 and 877 Judicial Code*
 - Sanction: *Art. 882 Judicial Code*
 - But: lawful reason: e.g., duty of professional confidentiality: *Art. 882 Judicial Code*

Special regulation re e-information

- Criminal acts
 - Falsification in IT
 - IT fraud
 - Criminal acts against confidentiality, integrity and availability of IT systems and of data saved, processed or transmitted through these

Special regulation telecommunication company

- Law e-communication
 - Rule: removal obligation after communication (art.122)
 - Exception:
 - Invoicing
 - Until the end of the invoice dispute or judicial enforcement of payment
 - Marketing
 - Without prejudice to Privacy Law
 - Fraud investigation
 - Communication criminal act to competent authorities

Special regulation telecommunication company

- Law e-communication
 - Rule: obligation to store (art.126 – old art. 109 ter, E Law 21.3.1991)
 - Traffic data
 - Identity data
 - Purpose: investigation and punishment criminal acts
 - Min. 12 months - Max. 36 months
 - Royal Decree is required
 - Directive 2006/24/EC
 - » Not transposed yet
 - » Categories data (art. 5, a - f)
 - » Not the content
 - » Min. 6 months – Max 2 years
 - Draft Law and Royal Decree

Special regulation telecommunication company

- Obligation to cooperate
 - With the Public Prosecutor: art 46 bis Code of Criminal Procedure
 - identification
 - With the examining magistrate: art. 88 bis Code of Criminal Procedure
 - call data
 - With the examining magistrate art. 90 quater Code of Criminal Procedure
 - tapping content
 - Royal Decree 9.01.2003
 - Creation of a Justice Coordination cell

Electronic Data in Antitrust Investigations

- Leniency application
 - Company needs to review email accounts of employees to understand scope and nature of infringing activities and provide ‘added value’ evidence

- Request for information
 - Request for copies of specific emails of former employees going back until 2002 and comments on the context thereof

- Dawn raid
 - Investigators take full copy of email account of several employees including in house counsel

Leniency application

- Legal basis for processing of employee personal data:
 - Consent
 - Balance of interests
 - CAO/CCT 81?

- In practice : consent forms

- Legal hold instruction

Request for information

- Legal basis for processing of employee personal data:
 - Consent
 - Legal obligation
 - Balance of interests
 - CAO/CCT 81

- In practice : consent forms

- Legal hold instruction

- Legal Privilege issues

Dawn Raids

- Powers of investigators regarding electronic data
 - Take copies
 - Seize (not EU)
 - Seal
 - Use IT/forensic experts
- Legal hold instruction
- List search terms used and documents copied

Dawn Raid Incidents

- Privacy is no excuse
- The full mailbox incident
 - Scope of the investigation
 - Legal privilege
 - Outside counsel
 - In house counsel

Dawn Raid Incidents

- Case law & Guidance:
 - Madrid, September 30, 2009
 - Cass. Fr, January 26, 2011

Dawn Raid Incidents

- Case law & Guidance :
 - Akzo :
 - Provide reasons for claim
 - Cursory look (heading, layout, title, ...) unless this reveals content
 - Sealed envelope
 - Commission Decision
 - Appeal General Court

 - « Werkwijze Nma analoog en digitaal rechercheren » (2010)
 - Search terms
 - Separation of data « within scope » and « possibly outside of scope »
 - Sealed envelope in case of disagreement
 - Analysis by « functionaris verschoningsrecht »
 - No access by case team before decision by « functionaris »

Procedure for Dealing with Incidents

- Belgium:
 - Sealed envelope
 - Decision by other Auditeur
 - Appeal with the Competition Council

Legal Privilege

- Outside Counsel
 - Akzo :
 - Includes preparatory documents drawn up exclusively for the purpose of seeking external legal advice
 - Mere fact that document was discussed with outside counsel is not enough
- In House Counsel
 - Akzo : in house counsel excluded
 - « ... as a result of the in-house lawyers economic dependence, and the close ties with his employer, that does not enjoy a level of professional independence comparable to that of an external lawyer »
 - Belgian investigations :
 - Letter Auditorat April 10, 2008
 - Application in practice

Sanctions

- Fines & periodic penalty payments
 - Belgium :
 - Fine : 1% of yearly Belgian turnover for obstruction
 - Astreinte/Dwangsom : 5% of average daily turnover
 - Europe :
 - Fine : 1% of total turnover
 - Periodic penalty payments : 5% of average daily turnover
- Examples :
 - EON : € 38 million (breach of seals - EC) = 0,14%
 - J&T : SO (failure to block an email account, failure to open encrypted emails, diversion of incoming mails – EC)
 - Bambino : € 2500 (insufficient cooperation – BE)

Be prepared !

- Prepare adequate email usage policies and obtain necessary privacy consents in advance
- Prepare and enforce a data retention policy
- Prepare and enforce rules with respect to marking documents as legally privileged, forwarding legally privileged documents and storing legally privileged communications
- Prepare dawn raid policy and standard language for legal hold

e-Discovery in the U.S.

- Why does a Belgian company care?
 - Broad reach of U.S. jurisdiction in civil litigation
 - Discovery of corporate subsidiaries, affiliates, joint ventures
 - Third party discovery of customers, suppliers, agents, etc.
- The story of Dexia

Scope of US Discovery

- Extremely broad: “Relevant” or potentially relevant to the claims, defenses or issues in the litigation
- Specifically includes all “electronically stored information” (ESI)
 - email, e-docs (wherever stored)
 - databases, shared files
 - websites, social network sites
 - blackberries, PDAs, voicemail
 - metadata, hidden data
- ESI must be produced in electronic, searchable form
- And ... the producing party pays the costs for its own information

Discovery Obligations Begin Early

- Duty to preserve: triggered when party “reasonably anticipates” litigation
- Requirement to preserve all information (including ESI) potentially relevant to litigation
 - Issue legal hold notices
 - Cease automatic deletion of relevant electronic information, such as:
 - Email autodelete
 - Dynamic databases
 - Backup tapes or archival systems

Discovery Process – Emerging Law

- Requirement to “meet and confer” with opposing party regarding preservation and discovery of ESI
- Use of search terms and culling technologies
- Format of production
- Privilege issues
- Authenticity and admissibility

Failure to Comply = Sanctions

- Discovery about the discovery (e.g., depositions, motions, hearings)
- Sanctions could include:
 - Costs
 - Additional discovery
 - Adverse inference instructions
 - Preclusion of evidence
 - Dismissal of claims or judgment in favor of non-spoliating party
- Big factor is whether the “spoliation” was negligent, grossly negligent or intentional
- Proportionality and reasonableness are increasingly considered by courts

U.S. Discovery vs. Foreign Data Privacy Laws

- Vastly different notions of privacy and “personal data”:
 - U.S.: Medical records, banking records, social security numbers
 - EU: *Any* information relating to an identifiable individual (e.g., signature block on email)
- Between a rock and a hard place:
 - Court order in U.S. litigation vs. blocking statues in other countries

U.S. Courts Generally Have Not Been Accommodating

- *Société Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for the S. Dist. Of Iowa*, 482 U.S. 522 (1987).
 - Seminal Supreme Court ruling regarding a personal injury suit in Iowa against airplane manufacturers in France
 - Defendants sought protective order because of French blocking statute and argued plaintiffs should have to use the Hague Evidence Convention
 - Court held: Hague Evidence Convention is *not* exclusive or mandatory method for obtaining evidence abroad
 - Court held: “It is well settled that such [blocking] statutes do *not* deprive an American court of the power to order” a party to produce evidence

Recent Trends in U.S. Cases

- *In re Grand Jury Subpoenas (LCD Antitrust Litigation)*, 627 F.3d 1143 (9th Cir. Dec. 7, 2010)
- *In re Payment Card Interchange Fee and Merchant Discount Antitrust Litigation*, 2010 WL 3420517 (E.D.N.Y. Aug. 27, 2010)
- *In re Air Cargo Shipping Servs. Antitrust Litigation*, 2010 WL 1189341 (E.D.N.Y. March 29, 2010); 2010 WL 2976220 (E.D.N.Y. July 23, 2010)
- *Gucci America, Inc. v. Curveal Fashion*, 2010 WL 808639 (S.D.N.Y. March 8, 2010)
- *Accessdata Corp. v. ALSTE Technologies GmbH*, 2010 WL 218477 (D. Utah Jan. 21, 2010)
- *In re Global Power Equip. Group*, 418 B.R. 833 (D. Del. Oct. 28, 2009)

Other Recent Developments in Cross-Border Discovery

- The Sedona Conference
 - Working Group 6 focuses on international e-discovery
 - August 2008 “Framework for Analysis of Cross-Border Discovery Conflicts”
 - Sept. 2009 (Draft) “Best Practices, Recommendations & Principles for Addressing the Preservation and Discovery of Protected Data in U.S. Litigation”
- EU Article 29 Data Protection Working Party – the EU’s independent advisory body on European privacy and data protection law
 - February 2009 Paper (WP 158) on “pre-trial discovery for cross border civil litigation”– with invitation to The Sedona Conference to comment
 - October 2009 “Comment of The Sedona Conference Working Group 6 to Article 29 Data Protection Working Party Working Document”

Best Practices

- Have a plan in place for implementing legal holds
 - You can fight about what has to be produced later, as long as the information has not been destroyed
- Consider options for limiting scope of what must be produced
- Consider options for minimizing conflicts with data protection provisions
 - De-identification of personal data
 - Consent/notice of data subjects/authors
 - Consent of data commissioner
- Stipulations and protective orders to:
 - Provide adequate safeguards for protected data
 - Permit time for adequate processing and transfer
 - Establish reasonable methodology for processing and transfer

Questions?

fpetillion@crowell.com
tdemeese@crowell.com
jthomas@crowell.com

Tuesday, 8 February 2011