GLOBAL FORUM 2006

SECURITY AND PRIVACY : THE ODD COUPLE ?

Laurent Szuskin
Attorney at Law
laurent.szuskin@lw.com
Paris Office

LATHAM&WATKINS

When Privacy meets Security…

- "[…] *While acknowledging the legitimacy of the security interests at stake, the* [European] *Commission informed the United States authorities,* […] *that those* [US Fed. Statutory] *provisions* [on communicating PNR data to the CPB] *could come into conflict with Community and Member State legislation on data protection* […]"

  - (Judgment of the ECJ, May 30, 2006, annulling the EU Council and Commission decisions supporting the US/EU agreement on the transfer of PNR data)

Causes for annulment and next steps

- Inappropriate legal basis used by Council and European Commission to authorize such agreement (hence, subsequent personal data processing and transfers)
- Relevant processing outside of 95/46 EC Directive and, more generally, outside of Community law:
  - Processing related to public security and activities of the State in the areas of criminal law
  - Consequence : need to ground the agreement either on national laws or other EU community law pillars
- WP 29 issued opinion 5/2006 in June 2006, urging to maintain and improve level of protection of passengers rights
- Interim agreement apparently found in mid-October

In a convergent environment, is privacy an obstacle to security?

Measures taken for the purpose of enhancing security of people, goods or transactions, on electronic communications networks, may sometimes be dismissed or criticized on the ground of prevailing privacy principles

Three examples

1. The monitoring of SWIFT electronic networks: recent critics raised notably by the EU Commission and the Belgian Personal Data Authority

2. The prohibition of certain transborder data flows from the EU to certain Third countries, save exceptions

3. The difficulty to implement certain antipiracy measures on Internet

The SWIFT case

- During years, the CIA and the US Department of Treasury have monitored transactions on SWIFT electronic networks, with the cooperation of SWIFT, including personal data
- In July 2006, the EU Commissionner for Liberty, Security and Justice, stated that such process could violate national laws protecting personal data
- In September 2006, the Belgian Data Protection Authority stated that SWIFT had violated Belgian law protecting personal data
- WP 29 is expected to issue a statement reflecting the position of EU Data Protection authorities, concurring with the Belgian one

Is the issue how the situation was handled, rather than the situation itself, in this delicate field?

Prohibition of certain transborder data flows

- Transfer of personal data to (data controllers and/or subcontractors located in) certain third countries which are considered by the European Commission as not providing *sufficient level of protection* are prohibited

- However, are not deemed a « transfer » subject to this rule:

  - Posting personal data on an Internet webpage, even if this posting renders such personal data accessible worldwide
    - (**ECJ, "Lindqvist", Nov. 6, 2003**)

  - Communicating personal data over the Internet to an ISP established outside the EU (unless the ISP "makes use" of local means of processes, other than for transit purposes)
    - (**see WP29, May 29, 2002 Working Document on determining the international application of EU data protection law to personal data processing on the internet by non-EU based web sites**)

Exceptions to this prohibition (non exhaustive…)

- Furthermore, there are limited and strict exceptions to this prohibition, including – but not limited to -- when:
  - The EU Commission takes an "Adequacy Decision", as in 2000 with the *Safe Harbor* framework – US companies may self-certify compliance to principles enforced by the US Department of Commerce and the FTC
    - **list: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm**
  - Multinational groups of companies implement Binding Corporate Rules
    - **WP29 working docs. of 4/14/05 on the (i) "model checklist" application for approval of binding corporate rules and (ii) cooperation between authorities**
  - EU and foreign Data Controllers and/or Sub-Contractors agree to (EU standard or *ad hoc*) contractual provisions protecting personal data
    - **controller to controller: Commission Decisions 2001/497/EC and C(2004)5271; controllers to subcontractors: Commission Decision 2002/16/EC**
  - Obtaining express consent from Personal Data subject
    - **"Transferts de données à caractère personnel […]" (CNIL), 01/06, p. 28 to 30**

Antipiracy measures on the Internet

1. Principle: prohibition to "private" monitoring of Internet to fight peer to peer (*i.e.*, under criminal and merely civil – torts or (with a nuance) breach of contracts -- theories)

2. Exception: article 9-4 of the French Data Protection Act:
   - Processes « *relating to offenses* […] » may only be implemented by certain legal persons (e.g., collecting societies, professional defense organizations) and are subject to the CNIL's prior approval
     - **The Constitutional Council, in Decision n° 2004-499, struck down a legislative provision allowing a broader right to private monitoring**

3. Examples: the SACEM (refusal) and SELL (approval) CNIL Decisions

In a convergent environment, is security an obstacle to privacy?

Sometimes, the objective of security must prevail over personal data protection principles – provided that a balance is found

Four examples

1. Implementation of certain DRMs
2. Monitoring of electronic communications – traffic and other data
3. Set-up and sharing of (financial) black lists / white lists
4. Sanctioning identity theft

DRMs

- "DADVSI" Code (Act of August 1, 2006), article 15:
  - If DRMs permit the remote control of functionalities or access to personal data: need of prior formalities with:
    - ✓ CNIL (regulatory authority on personal data)
    - ✓ Security and Encryption Department (encryption matters) – incl. providing a copy of the source code
  - Implementing Decrees are expected

Electronic communications – traffic and other data

- **Principle: L 34-1 of the Post and Electronic Communications Code:**
  - IAP and other persons which activity is to offer access to electronic communications services to the public must erase or render anonymous traffic data (see also: Decree n°2006-358 of March 24, 2006)
- **Exceptions (non limitative) – but n/a on "contents" of communications:**
  - 1 year postponement is possible to evidence and trace criminal acts and for the sole purpose of making such information available to judicial authorities
  - Electronic communications operators can use and store billing and payment data for the purposes of recovering receivables (and for the legal duration applicable thereto) and to market their services (complying with the French "anti spam" legislative provisions) as well as other data to ensure network security
  - To fight terrorism, certain police members may also access to certain traffic and other technical data

(financial) black lists / white lists

- Article 25 of the French Data protection Act: prior approval from CNIL is required if process of personal data may exclude persons from benefit of a right, service, or a contract (*e.g.*, Preventel) absent a legislative right to this effect

- Only the *Banque de France* may hold the central register of credit, checks and credit card incidents; access to it is limited and conditional
  - **see CNIL "black lists" report, CNIL web site**

- Certain want to introduce white listing – *e.g.*, credit bureaus -- but the CNIL is highly reluctant to it
  - **see CNIL "white list" ("centrales positives) report, 2005, CNIL web site**

Identity theft

- Fraudulent use of a third party's identity is not *per se* criminally sanctioned, except in specific cases
- There is some French case law sanctioning identity theft on the Internet which supported criminal acts, e.g., for "*voluntary violence with premeditation*", fraudulent access to IT system, etc.
- A bill was introduced in July 2005 before the Senate to punish *per se* the fraudulent use of a third party's identity. It is still pending
- However, on October 19, 2006, the French Chief Justice stated at the Parliament that existing legislation sufficiently encompassed identity theft and that no change was necessary

SECURITY vs. PRIVACY: A GLOBAL DIVERGENCE?

"We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government"

ATTRIBUTION: Justice **WILLIAM O. DOUGLAS**, dissenting, Osborn v. United States, 385 U.S. 341 (1966)

- It is legitimate to maintain and increase security on – and of -- electronic networks and digital contents, to protect the people, their goods, transactions and rights from the inherent danger of doing business and other activities online
- It is no less legitimate that the search for security must not be at cost of privacy, which is also a tool to bring confidence in e-commerce
- The legislative and regulatory powers – and the courts – must find the right balance to protect both the "community" and the "individual" on -- and from -- their activity on electronic networks and services