Institute for European Studies
Vrije Universiteit Brussel

CENTER FOR LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES
AT THE VRIJE UNIVERSITEIT BRUSSEL
BELGIUM

Law, ethics and justice for preemptive security practices

Presentation at PRISE Final Conference
Vienna, 29/04/2008

Gloria González Fuster

Scope of the presentation

- Evolving security practices represent new challenges for law, ethics and justice.
- The evolution of security practices is globally marked by a trend towards preemptive security practices.
- Preemptive security practices might actually require a specific response by the law.
- Two main questions:

  - Need to rethink the right to privacy and the right to data protection?

  - Are other other legal responses need?

Preemptive security practices (I)

- Since 9/11, especially in the US, marked trend towards preemption.
- Preemptive security practices are deployed in different areas: anti-terrorism, but also crime-fighting, border control.
- Different degrees of preemption possible:
  - There is an identified threat.
  - There is a will to identify the threat itself:
    - Use of data mining to identify 'risky groups' by their different patterns of 'suspect behaviour': 'categories of suspicion' are created.
    - Falling under a 'category of suspicion' makes somebody suspect.
  - If there appears to be no threat, possibility to concentrate on identifying the risk of unexpected threats.

Preemptive security practices (II)

- They share a series of common features:
  - Massive collection / processing of data.
  - Use of data originally collected for other uses.
  - Processing of the data to define what is being looked for (creation of 'categories of suspicion' through data mining).
  - Further processing to identify those matching the profile.
- They rely on technology, different technologies.
- They are inscribed in a general dynamic.

Preemptive security practices (III)

- Office of the Director of National Intelligence (US Congress) February 2008 report on data mining: overview of US intelligence data mining development programs.
- Data mining: to discern patterns of activity that could indicate a threat to national security.
- Examples:
  - Video Analysis and Content Extraction (VACE),
  - Reynard: *social and 'particularly terrorist' dynamics in virtual worlds and large-scale online games*
  - Methodological research: allow constant assessment of threats to determine 'the threat likelihood of unexpected threat entities'

Examples of in the EU?

- Much discussed whether US approach has been adopted by the EU or not.
- Even if US approach only, the impact is relevant for the EU citizens (PNR).
- In the EU:
  - Support of the conditions enabling those practices: Data Retention Directive, interoperability.
  - Some concrete steps: 3rd Money Laundering Directive('preventive effort').

An example: EU PNR-system (I)

- Draft Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, proposed November 2007.
- Background: in March 2004, the Council invited the EC to bring forward a proposal for a common EU approach to the use of passenger data for law enforcement purposes. The Hague Programme also invites the EC to do so.
- The draft Framework Decision prescribes obligations relating to the handling of PNR data to be undertaken by the Member States in relation to air carriers operating flights to or from the territory of one or more of the Member States.
-

An example: EU PNR-system (II)

- Airlines collect passenger data for commercial purposes.
- Member States designate Passenger Information Units to collect the PNR data from the airlines.
- The Unit carries out risk assessments of passengers "*in accordance with criteria and guarantees provided for under national law*" (to be determined).
- Data are processed for the purposes of preventing or combating terrorism or organised crime, including:
  - To identify persons or their associates who may be involved in such offences;
  - To update risk indicators.
- After the assessment, two possibilities:
  - Passenger falling under 'high risk' category: extra inspection.
  - Passenger not under 'high risk' category: normal surveillance.

Impact on law, ethics and justice

- Impact on privacy and civil liberties of data mining for preemption is widely acknowledged: i.e., because of the impact of data mining on privacy and civil liberties, IARPA [the Intelligence Advanced Research Projects Agency] in US is also investing in projects that develop privacy protecting technologies.
- Impact is actually wide, cannot be covered by technology only.
- Main ethical issues: everybody is co-opted to work for law enforcement: no choice.
- Justice problems, especially discrimination:
  - Calls have been voiced for 'neutral' profiling, but how 'neutral' can be a procedure designed to sort people out?
  - Inequality of quantity of data available.
  - Legitimacy of power.

Re-thinking data protection? (I)

- The right to privacy and the right to the protection of personal data have clear, distinct roles to play:
  - Privacy : negative (protection)
  - Data protection: positive (user control, self determination)
- Ensuring that they are respected and implemented should not be an obstacle to question them: need to a debate on their validity after the shift to preemption.
- Historically, the right to the protection of personal data grants the citizen a series of subjective rights, based on a series of principles:
  - Legitimacy
  - Proportionality
  - Purpose binding
  - Transparency
  - Security of the data
  - Quality of the data: accuracy principle: data accurate and up to date

Re-thinking data protection? (II)

- General assumption: Problems related to 'quality of the data' are an obstacle to the deployment of preemptive security practices.
- 'Quality of the data': a responsibility for the data controller.
- 'Data accuracy': a subject right or a structural limit to the right to the protection of personal data? (Article 8(2) Charter: "*Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".*
- Problems of general assumption:
  - Would accurate data guarantee fair automated decisions? (see i.e. French 1978 law prohibiting automated decisions)
  - Other obstacles: i.e., heterogeneity of data
- The right to provide inaccurate data as a privacy enhancing right? No real 'user control' without freedom to determine degree of accuracy.
- Ethical choices are then possible.

Privacy and data protection not enough

- The right to privacy and the right to data protection need to be ensured for those whose data is processed. Specific problems are to be solved requiring detailed consideration to ensure effective implementation of legal requirements.
- However, the right to privacy an the right to data protection are not the only fundamental rights at stake.
- Most of preemptive security practices mark a shift in the 'presumption of innocence' principle.
  - Not all. Predictive data mining and profiling techniques are not problematic per se: their use does not convey the same concerns in certain practices, i.e. applications carrying out evaluation of offenders in order to define their profile and assess the risk of re-offending.
- New status needing special protection: Those (for the moment) innocent identified as following under a 'category of suspicion'

The rights of the suspect(s)

- From the 'right of the suspect' to 'the rights of suspected categories'.
- PNR example: the 'rights of the high risk passenger', including redress and compensation.
- ECJ cases useful: court review of ius cogens in terror blacklisting cases (i.e. Kadi and Yusuf). Concretely on the rights of the defense and the right to effective judicial protection.
- Due process: right challenge decisions.
  - Main issue: The construction of categories should be transparent enough to ensure accountability.

Institute for European Studies
Vrije Universiteit Brussel

CENTER FOR LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES
AT THE VRIJE UNIVERSITEIT BRUSSEL
BELGIUM

Thank you.

Gloria.Gonzalez.Fuster@vub.ac.be