Data protection in the EU & in EU-US relations: A dangerous blurring of boundaries between the use of information for criminal investigation purposes and state security purposes?

Rio State University | Law Faculty
Rio de Janeiro | 13 November 2013
international

• expert participation in EU troika meetings US state in October 2011
• European Commission research projects
• Europol/Council of the EU working groups

national

• national research projects
• privacy commissioner @ Belgian Data Protection Authority
  • directly involved with Swift & Bics cases and with EU data protection policy
• PhD on EU-US infoex in criminal matters (2010) (annex 1)
Approach

law enforcement in the EU: information exchange

• within respective MS
• between MS
• between EU bodies/agencies and 3rd countries/organisations
• between MS and 3rd countries

traditional purpose of law enforcement = criminal investigation, aimed at bringing justice

• traditionally: by & between judicial police & justice actors
• vs administrative-governmental-military-political purpose
  • including intelligence activity
where infoex for law enforcement purposes

- allows/institutionalizes bypassing of criminal procedural guarantees
- leads to purpose deviation/is based on hollow purpose limitation or speciality principles
- is based on rules disrespecting fundamental principles
- is left merely control, monitoring, eminent person oversight etc

application

- in the EU internally
- in 3rd states/organisations (case: US internally)
- between EU and 3rd states/organisations (case: EU-US)
EU internally (pre-Lisbon)

13 Nov 2013 | Rio State University | Data protection in the EU & in EU-US relations: A dangerous blurring of boundaries between the use of info for criminal investigation & state security purposes?

directive 95/46/EC (Article 29 Working Party, Council of the EU)
• Article 3: non-applicable to police/justice/criminal law (3rd pillar)
• but implemented into that area by certain MS (including Belgium)
• and: 1st pillar (commercial) data are relevant for law enforcement
• Safe Harbour (self-regulation)

2000 EU MLA Convention (telecom interception)
intelligence services break-in to Europol, SISII, VIS, etc
OLAF investigations
data retention telecom data, EU-PNR + 2006 & 2009 ECJ cases
framework decision 2008/977 data protection 3rd pillar
• existing specific regimes/agreements unaffected
• only limited guarantees for further transfer to 3rd states
• transfer own information to 3rd states not covered
• assessment adequate data protection level: per MS (full discretion)
general institutional changes

data protection as a subjective right

• Article 8 EU Fundamental Rights Charter (text)
• Article 16 TFEU (text) - consequences for existing instruments
  • directive 95/46: to be replaced by generally binding regulation!
  • framework decision
    • obligation to adopt new instrument (directive)
    • new framework must also cover
      • domestic information exchange
      • transfer own information to 3rd states
    • all other non-data-protection specific instruments (none)
General institutional changes

pillar structure not totally abandoned (unlike European Constitution)
- TEU (former 2nd pillar) & TFEU (former 1st and 3rd pillar)
- (slight) domain-specific differences retained in TFEU
- including for: area of freedom, security and justice (AFSJ)
  - Title V TFEU – umbrella chapter for reunited JHA domains

single set of legal instruments (including in former 3rd pillar matters)
- regulations and directives
- full introduction supranationality for police/justice/criminal law

ordinary decision making process for former 3rd pillar (exceptions)
- co-decision (examples)
- qmv (exceptions) + emergency break
- right of initiative: Commissom (NB 2 commissioners) or ¼ of MS

<<<
1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.
TFEU (Article 16)

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.
adequacy data protection level?
safe harbour/not checked/assessed by individual MS, whilst
• inter-agency-sharing
• use for any purpose
• administrative subpoenas (separation of powers?)

Foreign Intelligence Security Act
• non-warranted capturing broadened by Patriot Act changes
EU in relation to US | Pre-Lisbon

13 Nov 2013 | Rio State University | Data protection in the EU & in EU-US relations: A dangerous blurring of boundaries between the use of info for criminal investigation & state security purposes?

unaffected unless decided otherwise

- PNR EU-US
- Swift (history)
EU in relation to US | Post-Lisbon

13 Nov 2013 | Rio State University | Data protection in the EU & in EU-US relations: A dangerous blurring of boundaries between the use of info for criminal investigation & state security purposes?

- Swift – remaining problems
  - distinction intra-EU and other transactions
  - bulk transfer (cfr pull-push discussion PNR)
  - inadequacy US data protection regime
  - only relates to law enforcement data (not: all LE relevant data, like PNR, telecom and banking data, …)
  - no solution for purpose deviation + …
• Snowden: no real surprises, but
  • magnitude of data capturing/espionage practice
  • bypassing of official EU-US agreements (e.g. Swift)
  • predominantly intelligence services-led (NSA)
• political consequences for EU policy making
  • difficult issue (free trade agreement EU-US pending)
  • general political awakening (finally)
  • especially Commissioner for Justice envisages changes
    • data protection = fundamental right; no bargaining; no price to be paid
    • Evaluation ‘Safe Harbour’ announced end ’13
    • self-regulation (including BCR’s) insufficient
    • extra guarantees for EU citizens’ data in US?
• further logical consequences (revision PNR, Europol-US agreement, TFTP2 ...