US access to Cloud data: the human rights dimension

Gordon Nardell QC
Barrister, England & Wales

gordon.nardell@39essex.com

ThirtyNine
ESSEX STREET

The issue

- Post 9/11 legislative developments in US, culminating in the Foreign Intelligence Surveillance Amendments Act 2008 ("FISAA"):
  - Allows US authorities to access data relating to "non-US persons" held in remote computing systems – the Cloud!
  - Gives the authorities broad and barely constrained discretion to obtain and examine data, without warrant and with minimal safeguards for data subjects
- To date, response to powers of US legal regime in EU legislative context (including DP reform package) focused on familiar Safe Harbor system – "adequacy" etc.
- Is that compatible with ECHR Art 8 and EU Charter Arts 7/8?
- How will/should the answer shape the EU legislative response? What are implications for Member States/data subjects/service providers?

ECHR Article 8: the groundrules #1

- The wide net of privacy:
  - Interception of communications and access to personal data by State authorities raises an Art 8 issue
  - In cases of clandestine State activity, ECtHR prepared to treat mere existence of law as a sufficient "interference", at any rate if "reasonable likelihood" that measures have been applied to applicant. *Klass v. Germany* (1979-80) 2 EHRR 214
  - So most of the relevant cases concern compatibility of the law itself with Article 8

- Interference must be "in accordance with the law"…
  - Predictable and accessible: in clandestine interception cases, law must be "particularly precise", setting out "clear, detailed rules" on "categories of people" subject to measures, duration, procedures to be followed, rules on disclosure, etc. Must also contain adequate and effective guarantees against abuse: *AEIH and Ekimdzhien v. Bulgaria*, 28.6.07
  - Also applies to "strategic" monitoring involving collection of large, untargeted volumes of data from which information of interest is subsequently extracted by minimisation/filtering: *Liberty & others v. UK* (2008) 48 EHRR 1 (category of "everybody"!)
  - Extends to storage/access to private data even if not "clandestine" in sense that State practice widely known: *S. & Marper v. UK* (2009) 48 EHRR 50

ECHR Article 8: the groundrules #2

- ...and “necessary in a democratic society”. A collection of principles.

- Proportionate to legitimate aim pursued:
  - Fair balance must be struck, but starting point is the right, subject to “exceptions which must be narrowly interpreted“: *Sunday Times v. UK* (1979) Ser. A
  - Court sceptical of “blanket and indiscriminate” measures that operate without regard to individual impact and characteristics: *S. & Marper v. UK* (2009) 48 EHRR 50
  - Reflected in different attitude to “targeted” and “untargeted” measures
  - *Liberty & others v UK* [64]: “*discretion granted to the executive for the physical capture of external communications was... virtually unfettered*”. Violation.
  - *Cf. Kennedy v. UK* 26839/05 18.5.10 – targeted interception: no violation

- Sufficient safeguards against abuse (overlaps with “in accordance with law”). In interception/access cases, ECtHR has (inconsistently) insisted on:
  - Warrant procedure – authorisation by judge or other sufficiently independent person. Independent oversight.
  - Clear definition of purposes for which data may be accessed/processed , and rules/procedures to ensure use of data proportionate to that purpose
  - Data security
  - Regular review of retention
  - Notice to affected person, at least after the event, and right to challenge

  See eg. *Weber and Saravia v. Germany* 54934/00, 29.6.06.[95]

Positive obligations

- ECtHR recognises that in some circumstances, State not only bound to refrain from actively infringing Convention rights, but it positively obliged to ensure that its law and practice adequately guards the citizen against the excesses of others.

- Emanates from ECHR Art 1 -- parties agree to guarantee Convention rights to everyone within their jurisdiction: *Young, James and Webster v. UK* (1982) 4 EHRR 38

- Art 8 especially fertile ground because of "respect" formulation: *X. and Y. v Netherlands* (1985) Ser. A 91. Large body of case law involving successful complaints that State has failed properly to regulate, or take effective enforcement measures, against private/commercial activity that impinges on private life: *López Ostra v Spain* (1994) 20 EHRR 277; *Guerra v Italy* (1998) 26 EHRR 357

- Court applies proportionality principle much as in an "interference" case. Special rules apply where the complaint would require the State to allocate resources. But in most cases, result the same whether the case is analysed as "interference" or "positive obligation": *Hatton v. UK* (2003) 37 EHRR 28, [119]

How do the rules respond to the counter-terrorist context?

- ECtHR recognises State "margin of appreciation", but reluctant to dilute of standards of Convention protection even in cases involving security measures aimed at overseas terrorist activity.

- Committee of Ministers *Guidelines on Human Rights and the Fight Against Terrorism* H(2002)4: "*Within the context of the fight against terrorism, the collection and the processing of personal data... in the field of State security may interfere with... private life only if ... (ii) ...proportionate to the aim for which the collection and the processing were foreseen; (iii) ...subject to supervision by an external independent authority*".

- in *Liberty & others* Government relied heavily on international counter-terrorist context Court refused to accept this as justification for stark contrast between internal (targeted) and external (untargeted) interception regimes. Similar attitude of domestic courts applying the Convention. Eg
  - *A and others v. Home Secretary* [2004] UKHL 56 – House of Lords (precursor to Supreme Court) rejected discrimination between nationals/non-nationals in law establishing anti-terrorist "control orders" .
  - Constitutional Court decisions in Bulgaria, Romania, Germany, CZ *et al* on transposition of DR Directive

Interplay between ECHR and EU privacy law

- In general terms, ECHR and EU fundamental rights principles march in step – eg. *Österreichischer Rundfunk* C-465/00, CJEU

- Trend reinforced by the Charter:
  - Preamble affirms "*rights.... as they result ... from the case law of the CJEU and of the ECtHR*"
  - CJEU on Charter Arts 7 and 8 similar to ECtHR on ECHR Art 8: *Schenke v Land Hessen* C-92/09, C-93/09, CJEU (proportionality).
  - Prospective EU accession to ECHR.

- Judicial and legislative cross-fertilisation between European data protection principles and ECHR Article 8:
  - Convention 108 referred to in Art 8 case-law: *Amann v. Switzerland* (2000) 30 EHRR 843; *S. & Marper v. UK* (2009) 48 EHRR 50
  - Art 8 and case-law referred to in DP materials – WP29/EDPS reports etc

- Short point: answer likely to be the same under the two systems

How does FISAA measure up?

- Hard to know where to start...
  - Warrantless interception/access to a huge volume of material.: any data passing into/out of, and processed/stored in, the Cloud
  - S. 702 as amended refers to “targeting” – but refers to generic category of “persons reasonably believed to be located outside the US”, not to specific individuals who are suspected (reasonably or otherwise) of wrongdoing.
  - Purpose – acquiring information “*with respect to a foreign-based political organisation or foreign territory that relates to the conduct of the foreign affairs of the US*” -- hopelessly broad. Questionable whether a legitimate aim at all in Art.8(2) terms; could cover any political or purely private activity so long as it“ relates to” US foreign policy. Not tied to crime, public safety, national security, etc.
  - No notice to data subject. No remedy since right to judicial review is confined to the service provider, and fall-back of Fourth Amendment unavailable to non- US nationals with no link to US. Extends retrospective civil immunity of providers in relation to pre-FISAA warrantless wiretapping.
  - In that respect law discriminates between “US” and “Non-US” persons. As it does in relation to scope of information that can be acquired: “relates to” (cf. “*necessary to... national defense.. or conduct of foreign affairs.*

Implications for EU/ECHR States?

- No general responsibility of a Convention/EU State for activities of Third State. Depends on whether it engages State's "jurisdiction" within Art 1

- Extraterritoriality a complex area:
  - State responsible under ECHR if its own conduct exposes individual to misconduct by the Third State – eg. extradition/deportation.
  - Generally requires clear and serious infringement of rights in the Third State: eg. Art 3 (*Soering v. UK* (1989) 11 EHRR 439).

- But different rules apply where a Convention State itself acts or legislates in a way that infringes rights of individual within its jurisdiction:
  - In that situation, no answer that State was required by an international treaty to act as it did: *Bosphorus Hava Yollari v. Ireland* (2005) 42 EHRR 1.
  - Exception is where the conduct in question flows from the State's membership of an international organisation, established by treaty, which protects rights in an equivalent manner to ECHR. Rebuttable presumption of compliance: *Behrami v. France* (2007) 45 EHRR SE85.

- No difficulty in principle that Art 8 generates positive obligation to secure protection of data from wrongful access. But may need to distinguish:
  - Data processed within US jurisdiction outside EU: uncertain whether positive obligation to prevent Cloud data entering US jurisdiction
  - Data processed within EU by service provider under US influence: stronger case for requiring State to go behind Safe Harbor/"adequacy" decision re FISAA

What happens next?

- Would be best to confront the problem with at EU legislative level. Will become a problem anyway when EU accedes to ECHR since the Union itself – not just individual Member States -- will become subject to positive obligations deriving from ECHR/Charter.
- Arguably any EU legislation/agreement perpetuating exposure of Cloud data to FISAA would in any event be classed as an interference with data subjects' Art 8 rights
- Meanwhile a challenge for data subjects. Prospect of proceedings in domestic courts? In CJEU?
- And a headache for service providers operating in EU who have no EU equivalent of FISAA immunity for complying with US insistence on providing intercept/access capability