Data Retention and Signals Intelligence

Dr. Mark Klamberg, Associate Professor

XXXI Nordic conference on Law and IT, e-Stockholm ’16, Secure Digitalisation
Outline

I. What is privacy?

II. Electronic surveillance
   • Data retention
   • Signals intelligence
What is Privacy?  
– a legal umbrella of concepts

Figure 1

Solove, A Taxonomy of Privacy, 2006
European convention for the protection of human rights

Legitimate interference under article 8 require:

1. Legal basis (and the law should be of a certain quality)
   • Accessibility
   • Predictability
   • "Rule of law"
2. Legitimate aims
3. Necessary in a democratic society
   • Proportionality

Similar requirements under articles 7 and 8 of the EU Charter
Changes in Our Society

Technological change
Until the end of the 1990s satellites were the main medium for international communication. Now it is fiber optics in cables controlled by private companies.

Shift in Threats Relevant for National Security
The perceived threat from the Soviet Union has been replaced with vague threats such as terrorism, international criminality, migration, environmental threats and financial imbalances. Comeback for “cold war” threat?

New Legal Demands
The European Convention on Human Rights requires that interferences in the private life and family has a legal basis (article 8)

Privatization
Telecom operators were previously state-owned and controlled. Now they are private companies whose priority is to safeguard the interests of their customers, not the interests of the state
## Four fields of legislation

<table>
<thead>
<tr>
<th>International communication</th>
<th>Domestic communication</th>
</tr>
</thead>
</table>

**Preliminary Investigation**

**Intelligence**
Data retention

CJEU judgment C-293/12 and C-594/12, Digital Rights Ireland et al., 8 April 2014

Temporary pause in data retention with leave of the Swedish Post and Telecom Authority (PTS)

Preliminary assessment 13 June 2014 that:
• Swedish Law was in compliance with the EU Charter (and other relevant EU law/principles)
• Need to consider whether prior independent review should be introduced in relation to Data Collection
• (see committee directive 2014:101)

Government inquiry SOU 2015:31:
Minor changes to the Data Collection Act, no change and no introduction of prior court review
Requests for a preliminary ruling from Kammarrätten i Stockholm (the Administrative Court of Appeal, Stockholm, Sweden), C-203/15

The following questions were referred to the Court of Justice for a preliminary ruling:

(1) Is a general obligation to retain data in relation to all persons and all means of electronic communication and extending to all traffic data, without any distinction, limitation or exception being made by reference to the objective of fighting crime [as described in paragraphs 13 to 18 of the order for reference] compatible with Article 15(1) of Directive 2002/58, taking into account Articles 7, 8 and 52(1) of the Charter?

(2) In the event that the first question is answered in the negative, may such a retention obligation nevertheless be permitted where:

(a) access by the national authorities to the retained data is governed in the manner specified in paragraphs 19 to 36 [of the order for reference], and

(b) the protection and security of the data are regulated in the manner specified in paragraphs 38 to 43 [of the order for reference], and

(c) all relevant data must be retained for a period of six months from the date on which the communication was terminated before then being deleted, as described in paragraph 37 [of the order for reference]?
Request for a preliminary ruling from the Court of Appeal (England & Wales) (Civil Division), C-698/15

The following questions were referred to the Court of Justice for a preliminary ruling:

(1) Does the judgment of the Court of Justice in Digital Rights Ireland (including, in particular, paragraphs 60 to 62 thereof) lay down mandatory requirements of EU law applicable to a Member State’s domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of the [Charter]?

(2) Does the judgment of the Court of Justice in Digital Rights Ireland expand the scope of Articles 7 and/or 8 of the Charter beyond that of Article 8 of the European Convention of Human Rights (“ECHR”) as established in the jurisprudence of the European Court of Human Rights (“ECtHR”)?

By decision of the Court of 10 March 2016, the two cases were joined for the purposes of the oral part of the procedure and the judgment.
Opinion of Advocate General Saugmandsgaard Øe, 19 July 2016 (para. 132)

Six requirements that must be satisfied in order for the interference caused by a general data retention obligation to be justified:

– the retention obligation must have a legal basis;
– it must observe the essence of the rights enshrined in the Charter;
– it must pursue an objective of general interest;
– it must be appropriate for achieving that objective;
– it must be necessary in order to achieve that objective;
– it must be proportionate, within a democratic society, to the pursuit of that same objective.
Article 15(1) of Directive 2002/58/EC and Articles 7, 8 and 52(1) of the EU Charter are to be interpreted as not precluding Member States from imposing on providers of electronic communications services an obligation to retain all data relating to communications effected by the users of their services where all of the following conditions are satisfied, which it is for the referring courts to determine in the light of all the relevant characteristics of the national regimes at issue in the main proceedings:

– the obligation and the safeguards which accompany it must be provided for in legislative or regulatory measures possessing the characteristics of accessibility, foreseeability and adequate protection against arbitrary interference;

– the obligation and the safeguards which accompany it must observe the essence of the rights recognised by Articles 7 and 8 of the Charter of Fundamental Rights;

– the obligation must be strictly necessary in the fight against serious crime, which means that no other measure or combination of measures could be as effective in the fight against serious crime while at the same time interfering to a lesser extent with the rights enshrined in Directive 2002/58 and Articles 7 and 8 of the Charter of Fundamental Rights;
– the obligation must be accompanied by all the safeguards described by the Court in paragraphs 60 to 68 of its judgment of 8 April 2014 in Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238) concerning access to the data, the period of retention and the protection and security of the data, in order to limit the interference with the rights enshrined in Directive 2002/58 and Articles 7 and 8 of the Charter of Fundamental Rights to what is strictly necessary; and

– the obligation must be proportionate, within a democratic society, to the objective of fighting serious crime, which means that the serious risks engendered by the obligation, in a democratic society, must not be disproportionate to the advantages which it offers in the fight against serious crime.
Summary of the legislation adopted 18 June 2008:

IT- and telecom operators are obligated to transfer all communication in cables crossing Swedish borders to nodes controlled by the State

The Defence Radio Establishment will intercept communication and collect data at the nodes (signal intelligence)
Key Features of the Swedish law and the operations of the Defence Radio Establishment

1. Mandate for Surveillance by the Defence Radio Establishment

2. Clients

3. Review Mechanisms

4. Scope of Surveillance
1. Mandate of the Defence Radio Establishment

Mandate to monitor

1. external military threats,
2. factors relevant for peacekeeping operations,
3. international terrorism and international organized crime
4. the development and proliferation of weapons of mass destruction and arms control,
5. external threats against infrastructure (for example against information and communication technology)
6. conflicts outside of Sweden that effect international peace and security and
7. counter-intelligence
8. international phenomena relevant for Swedish foreign-, security-, and defence policy (Government and diplomatic correspondence,?)
2. Clients (known)

1. The Government
2. The Government office
3. The Defence Forces
4. The Police, including the Security Service (SÄPO)
5. National Inspectorate of Strategic Products
6. Swedish Customs Service
7. Defence Materiel Administration Agency
8. Defence Research Agency
9. Civil Contingencies Agency

International Partners exist but unknown which those are. Could include NSA, GCHQ, BND, DGSE and FE

Excluded in Autumn 2009
3. Review Mechanisms

1. Defence Intelligence Court
   • Reviews applications for surveillance missions in advance
   • Professional judge and politically appointed lay-members representing the majority and the opposition in Parliament
2. Defence Intelligence Committee
   • Reviews, *inter alia*, the integrity and use of the databases held by the Defence Radio Establishment
   • Composed of a legal professional and politically appointed lay-members representing the majority and the opposition in Parliament
   • Reports to the Government
3. Internal oversight board inside the Defence Radio Establishment
4. Ombudsman who report cases of misuse to the Parliamentary Ombudsman (JO) or the Chancellor of Justice (JK), (proposal)
5. Extraordinary review presented 2011 by the Data Protection Authority and a parliamentary committee
4. Scope of Surveillance

1. Fairly small amounts of messages are intercepted and processed
   Example from Germany, judgement of the First Senate of 14 July 1999, para. 89:

   The capacity of the Federal Intelligence Service (BND) permits the screening of approximately 15,000 acts of telecommunication per day out of a total of approximately 8 million telecommunications contacts between Germany and foreign countries. The material and personal resources of the Federal Intelligence Service, however, are not sufficient to evaluate all contacts.

   Approximately 700 fall under the area of application of the G 10 Act. Only these acts are selected with the help of the search concepts.

   About 70 of them are examined more closely by employees of the Federal Intelligence Service.

2. Traffic data (meta data) relating to all or large amounts of communication is stored by the Defence Radio Establishment in a database (Titan)
   Example from the USA: The NSA Call database contains 1.9 trillion records which include the records of tens of millions of Americans
Questions?
Thanks!

Follow me
Twitter: @klamberg
Blogg: www.klamberg.se