Statewatch

The "principle of availability"

- the free market in access to data/intelligence will rely on "self-regulation" by the law enforcement agencies and make accountability almost meaningless

Tony Bunyan, December 2006[1]

"With effect from 1 January 2008 the exchange of ... information should be governed by conditions set out below with regard to the principle of availability, which means that, throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State..

The methods of exchange of information should make full use of new technology and must be adapted to each type of information, where appropriate, through reciprocal access to or interoperability of national databases, or direct (on-line) access, including for Europol, to existing central EU databases, such as the SIS"
"

This is how the "principle of availability" was defined in the "Hague Programme" (5 November 2004).

For a long time bilateral and multilateral agreements have been in place for law enforcement agencies in one EU member state to make requests to those in another EU state on specific cases. This is backed by the EU Convention on mutual assistance in criminal matters adopted on 23 August 2005[2]. The "problem" for the law enforcement agencies is that this procedure takes time, involves a formal request and sometimes judicial authorisation.

---

[1] This article has been updated after being published in CILIP 84, no 2, 2006 (Burgerrechte & Polizei): http://www.cilip.de

[2] Status to date: needed ratification by a majority of the first fifteen Member States to enter into force; ratified by eleven of them: Austria, Belgium, Denmark, Portugal, Spain, Finland, France, Sweden, United Kingdom, Germany and Netherlands; also ratified by Cyprus, Estonia, Hungary, Slovenia, Poland, Lithuania, Czech Republic and Latvia.

Prior to 2004 a number of EU databases had been established – the Schengen Information System (SIS), Europol's Index and Analysis systems, Eurodac and the Customs Information System (CIS). Even the Council was at times surprised by their growth, for example, a report on "3rd pillar information systems" in May 2003[3] looked at six databases. For "Schengen" the number of access points was recorded as follows:

"which N.SISes can be consulted (approx.!!!): 125,000" (exclamation marks in the original!)

And this was at a time when only 12 of the 15 EU states were in Schengen, soon there are to be 25 EU states plus Norway, Iceland and Switzerland - how many access points will there be then?

The "principle of availability"

The need to share/exchange information and data (including intelligence) was a common theme in G8 discussions in 2002 and 2003.[4] Initially the scope was to combat terrorism but this soon extended to organised crime as well and then crime in general. In 2004 the EU circulated a questionnaire (the same as the one drawn up by the USA for G8 states) on the use of special investigative techniques (communications surveillance, bugging, informers etc) and access to their product.[5] A key aspect highlighted in responses to the questions is that in a number of EU states, was the need for judicial authorisation both to gather and pass on data and intelligence. "Judicial authorisation" was spoken of as an "obstacle" to efficient cooperation between agencies - both internally and externally.

The "trigger" for formalising the "exchange" of information between law enforcement agencies was the European Council Declaration on 25 March 2004.[6] This followed the bombing of trains in Madrid on 11 March 2004.

The Declaration called for the:

"simplifying the exchange of information and intelligence between law enforcement authorities of the Members States"

This was one of many measures that the "Statewatch Scoreboard" found had little or nothing to do with combating terrorism.[7]

One of the Commission's responses to this instruction from the Council came on 16 June 2004 when it published a proposal: "Towards enhancing access to information by

---

[3] EU doc 8857/03

[4] G8 is comprised of the USA, UK, Germany, France, Italy, Canada, Japan and Russia.

[5] See "exceptional and draconian" analysis:
http://www.statewatch.org/news/2005/jul/exceptional-and-draconian.pdf

[6] No mention was made of security and intelligence agencies in a whole series of proposals.

[7] http://www.statewatch.org/news/2004/mar/swscoreboard.pdf

law enforcement agencies" (COM 429/4) including the proposal that national law enforcement agencies should have access to "European information systems", and another on the principle of availability.[8]

It was an easy step from the calls for the "exchange" of information and intelligence to the "principle of availability"

A note circulated by the Netherlands EU Council Presidency on 22 September, in advance of the 30 September – 1 October, Informal Justice and Home Affairs Council said:

"With effect from 1 January 2008, exchange of information in the policy fields pertaining to the area of freedom, security and justice must be based on the ***principle of availability"*** (emphasis added)[9]

It went on to say:

"priority must be given to granting mutual access to national databases".

From the first draft of the Hague Programme (11 October 2004) the "principle of availability" was set in stone.[10] At the European Council (Summit) on 5 November 2004[11] the Hague Programme was simply nodded through without debate - the Prime Ministers had other more important matters to discuss. *Statewatch* had put the first draft online on 18 October but there was little or no time for parliaments or civil society to comment or intervene.

It was a programme drawn up by officials and agencies, endorsed by Ministers and then Prime Ministers in secret meetings without any real democratic input. Thus was the justice and home affairs programme of the Council Presidencies and the European Commission for the next five years adopted.

In March 2005 the Luxembourg Council Presidency put forward a Note[12] on "efficient information exchange" to spell out the "principle of availability":

"The aim is obviously that as large a list of information categories as possible is exchangeable with as little effort as possible (ie: requiring a minimum of formalities, permissions, procedures, ***if any****)"* (emphasis added)

It advocated direct access to national law enforcement databases by other EU states on a "hit/no-hit" basis (DNA and fingerprints) and to:

---

[8] COM 429/2004:http://www.statewatch.org/news/2004/jun/com-429-infor-by-law.pdf and COM 490 (2005): http://www.statewatch.org/news/2005/oct/com-principle-availability.pdf

[9] EU doc no: 12680/04

[10] The European Parliament report of 29 September 2004 makes no mention of the "principle of availability" and its implications.

[11] An unfortunate date in British history - Guy Fawkes "bonfire night" remembering the man who tried to burn down parliament.

[12] EU doc no: 7416/05. Luxembourg was one of the Prum "seven".

"national administrative systems" ("registers on persons, vehicles, firearms, identity documents and driving licenses, as well as aviation and maritime registers)"

as well as to EU-wide databases.

On 27 May 2005 the Prum Treaty was signed by Germany, Spain, France, Luxembourg, Netherlands, Austria and Belgium (Italy has since said it wants to join too) and was thus "on the table" when the "Friends of the Presidency" (FoP) expert group were deliberating (see below). The Treaty covers a series of justice and home affairs issues.

The Prum Treaty nowhere uses the term the "principle of availability" instead preferring the "exchange of information" (ie: data and intelligence).

Articles 2-12 allow direct access by the law enforcement agencies in the other participating states to their databases on DNA, fingerprints and vehicle registration on a "hit/no-hit" basis.[13] In the event of a "hit" the file/personal data would be supplied. In the case of DNA (Article 7) where the requested state does not hold the DNA profile on the individual concerned it should be "collected" from the person. While for fingerprints access is granted not just for criminal prosecutions but also for "prevention" - with the law of the requesting state (rather than the requested state) being decisive.

"Friends of the Presidency"

A "Friends of the Presidency" (FoP) group of experts from the member states plus the General Secretariat of the Council and the Commission was set up in April 2005.

This allowed an EU initiative - that is, *within* the structures of the EU 25 member states as distinct from the "Gang of 7" agreeing the Prum Treaty - to develop the "**technical** modalities to implement the Principle of Availability" of the proposals in the Prum Treaty.

The FOP report was published on 24 October 2005 - but is only "partially accessible" to this day pages 4-41 are not public, that is, all the detail is deleted![14]

The FoP was asked to look in detail at six areas:

- DNA
- fingerprints
- ballistics
- vehicle registrations
- telephone numbers and communications data
- civil registers

On DNA, fingerprints and vehicle registrations it suggested enhanced cooperation via

[13] "Hit/no-hit" access would allow "fishing expeditions" to be carried out without any checks at all.

[14] EU doc no: 13558/05 and 13558/1/05 Rev 1, 10 November 2005:
http://register.consilium.europa.eu/pdf/en/05/st13/st13558.en05.pdf The full text is on:
http://www.statewatch.org/news/2006/nov/eu-fop-p-of-a-13558-rev1-05.pdf

direct access to databases. For ballistics and civil registers existing systems, with some improvements, were said to be satisfactory.

While concerning communications data it calls for:

"direct access to the relevant databases of the communications services providers within their Member States"

On communications data the FoP recommend *direct* access by LEAs to the information held by service providers rather than "indirect access on request".[15]

For DNA Interpol is a major sources to check profiles. The FoP supports the recommendation in the Prum Treaty for direct access by agencies in one country to the databases of other EU states on a hit/no-hit basis. In the long-term a "combined search engine" is proposed linking national databases and Interpol and "non-EU countries" - this would allow a "cold hit capacity" (an unexpected match without prior information).

Discussions following this report showed that some EU states do not have DNA databases (which they are urged to create). There are major differences however in the grounds for which DNA can be taken and retained. At one extreme the UK takes, and retains for ever, all DNA of everyone arrested - even if they are not charged or are acquitted. At the other, in many member states, DNA is taken for serious crimes of those convicted or suspected of them. Apart from the UK (6%) the number of DNA profiles held at national level in the EU is very small (around 1%) as a percentage of the population.

Access to fingerprint databases, which are much larger, should also follow the Prum Treaty with direct access on a hit/no-hit basis. And again a combined search engine is sought with the Interpol AFIS database. The FoP further says there should be direct access to EURODAC (fingerprints of asylum-seekers) and future biometric databases.

Vehicle registration data - vehicles and driving licences - is planned through EUCARIS (European Car and Driving Licence Information System) but only five countries are signed up so far. This will be overtaken by REGNET (vehicles) and RESPER (licences) - if agreed - and links provided to SIS and Interpol databases. After this report discussions on data protection have suggested that none is needed for these databases as this information is available anyway.

In its concluding remarks the FoP says that there is a:

"need to review procedures regarding judicial decision making in instances where it proves to be overly slow and cumbersome"

The Commission did not put forward its formal proposal for a Council Decision on the "principle of availability" until after the Prum Treaty and just two weeks before the

[15] However, the EU Directive on mandatory data retention by service providers agreed in December 2005 says traffic (communications) data must be kept by them and made available in ***specific*** *cases* for the purpose of law enforcement.

FoP report[16]. On 26 January 2006 the Commission sent a furious note to the Austrian Council Presidency[17] complaining about:

"the conclusion to postpone the discussion of the proposal for a Council Framework Decision on the exchange of information under the Principle of Availability"

At the same time the specific proposals in the Prum Treaty and the FoP report were being pursued with vigour with some member states pushing their own agendas. For example, France and Spain proposed, in a Note to the Article 36 Committee[18] that "notably for foreign nationals" there should be "surveillance of the entry and exit of third country nationals".

What conclusions might be drawn from these developments?

First, there is the undemocratic nature of EU policy-making. The Hague Programme which established the so-called "principle of availability" was not subject to parliamentary scrutiny by national or European parliaments nor was it available to the people and civil society to discuss and debate before it was adopted.

The same goes for the Prum Treaty which was developed and signed in secret governmental meetings - it now has to be ratified by the seven (maybe eight) national parliaments who will not be allowed to change a "dot or comma" - it is set in stone.[19]

What even more outrageous is that the Prum Treaty (yet to be ratified) is being referred to in the circles of EU Council working parties and committees time and time again as if it is part of the EU's justice and home affairs *acquis*.

Second, the "principle of availability" sweeps away external checks and controls over the exchange of information and intelligence (which may be "hard", based on fact or "soft", including that of dubious origin). In effect the agencies will be "self-regulated" with the all the dangers of misuse and abuse.

The law enforcement (police, immigration and customs) and security agencies will have unfettered access to any data held within the EU and, as is increasingly hinted at, with "friendly" non-EU states too.[20]

Third, the proposal for the principle of availability for law enforcement agencies came directly after the 11 March 2004 Madrid bombings – that is, as one of the responses to a terrorist attack. However, it covers *all* crimes or suspected crimes however minor

---

[16] COM 490/2005, 12.10.05.

[17] EU doc no: 5927/06.

[18] EU doc no: 9680/06, dated 22 May 2006.

[19] See "Behind closed doors" report by the House of Lords Select Committee on the EU: http://www.statewatch.org/news/2006/jul/hol-behind-closed-doors.pdf

[20] The US is already demanding - in secret meetings - access to information/data held on the Visa Information System EU, Passenger Name Record (PNR) and SIS II.

and is not targeted at combating terrorism.

Fourth, the "principle of availability" and data protection for the gathering, processing and passing on of personal data are absolutely irreconcilable. The draft proposal for a Directive on data protection on police and judicial matters is based on officials regulating themselves to decide whether or not data can be exchanged. The rights of the individual will be virtually non-existent, for example, where there is an ongoing investigation or national security (including public order) or it would prejudice relations with partners.[21]

Indeed the current discussions in the Council's working party on the draft data protection measure in police and judicial cooperation illustrates the theory that data protection is used more by the agencies to protect their own data than it is to give any rights to the individual.

Fifth, this leaves the situation that information and intelligence on an individual can be gathered in state A for one purpose, passed to state B for another purpose and further processed (added to) and then passed to state C (eg: outside the EU) where the same thing happens again with data passed around the agencies. How the individual is meant to get access to this "information trail" is nowhere considered in the data protection proposal. The accessing and processing of data/intelligence within the EU and outside – about which the individual will have no right to be informed – may well take on ominous implications with the growth of "watch-lists" (eg: to travel, financial transactions etc).

Finally, it might be thought that the reason for this explosion in the growth of state powers was 11 September 2001. In fact though 11 September was indeed the "trigger" for a swathe of new measures (as was 11 March in Madrid) the general direction had been determined much earlier by the Tampere Programme in October 1999. Under Tampere for the first time, in place of individual proposals put forward through the normal Council bodies by successive Presidencies, a 62-points comprehensive justice and home affairs programme was adopted at an EU Summit.[22]

The principle of availability and the "free market" in access to all (present and future) national or EU databases is a classic example of how EU governments have used the "war on terrorism" to give the emerging EU state sweeping powers of surveillance and control.

Tony Bunyan
December 2006

---

[21] Article 20 appears to suggest that the individual should be informed when data gathered on them is first disclosed to a third party but enquiries in Brussels brought the response that this would be down to existing national laws - when asked if any research had been conducted on national laws, the answer was no. See Statewatch's Observatory on data protection: **http://www.statewatch.org/eu-dp.htm**

[22] Like the Hague Programme there was no public draft until the final *adopted* plan was made available. Unlike the Hague Programme much of the detail in Tampere was actually decided at the meeting with many national "shopping lists" being circulated by national delegations.