Statewatch

Annotated guide to the issues and documentation on mandatory data retention in the EU

"If the security and intelligence agencies - who are at the forefront in stopping terrorist attacks - need access to the telecommunications data to be retained it is very hard to believe that EU governments would have taken over four years to come up with a proposal which will not come into effect for at least two further years. If this is the case they would be guilty of gross negligence and failure to protect the people of Europe. However, if additional powers are needed they should be strictly limited to dealing with terrorism and related offences."

1. The Council

Access by the law enforcement agencies to telecommunications data has been under discussion since 1993: See the **EU-FBI Observatory**, **SOS Europe** and **Statewatch database search for "data retention"**

Under the last Austrian EU Council Presidency in 1998 the infamous "**ENFOPOL 98**" (see: **EU governments to give law enforcement agencies access to all communications data - analysis**) was circulated, but the proposal was dead after widespread condemnation by civil society groups and individuals. This remained the situation until **Conclusions of the special meeting of the Justice and Home Affairs Council, 20 September 2001**. This was followed by the **George Bush's letter to the EU of 16 October 2001** which included the demand to:

"*Revise draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period."*

It took two and a half years for four member states (French Republic, Ireland, the Kingdom of Sweden and the United Kingdom) to put forward a proposal on 28 April 2004: **8958/05** (pdf). Between 28 April 2004 and 31 May 2005 six versions of the proposals were available on the Council's register of documents, eight were partially accessible ("PA", with the names of member states blanked out so that no-one could see what their governments were arguing) and one was not accessible. Between 1 June and 25 October 2005 there are no less than 13 substantive Council drafts, *none of which are publicly available on the Council's register of documents.*

The latest full draft of the Council's proposal, dated 10 October 2005: **12894/1/05** - this shows that there were major reservations by many member states on issues of substance. For example:

"In order to address the reservations in relation to Internet data, the Presidency had proposed a compromise package whereby "Internet chat" was included in Article 2(2) along with the wording proposed by FI ("provided by publicly available electronic communications service providers"). In conjunction with that, a "review clause" was inserted in Article 8. Several delegations (IT/HU/ES/CZ) could accept or supported the Presidency proposal. Others wanted to go further and include logs of web browsing, Internet chat and peer-to-peer communications (BE/SW/LT/DK). However AT/FI/LV/DE/FR/IE/GR/SK/EE could not accept the inclusion of Internet chat or other Internet data types expressing concern that the inclusion of such data might have an impact on the costs incurred and / or require more in-depth consideration in respect of a clear distinction between traffic data and content data which might risk delaying discussions. They thought that the outcome of the meeting of the Working Party in July 2005 reflected the minimum consensus and wanted to revert to that wording. The proposed review clause met with acceptance." (emphasis added)

However, despite this "compromise" Greece and Estonia maintained a "Scrutiny reserve" on the whole of Article 2 and Austria, Poland, Czech Republic, Cyprus, Slovenia, Latvia, Hungary and Finland maintained "Scrutiny reservations" on paragraphs 2-6 of Article 2.

The concern expressed by nine governments over "*a clear distinction between traffic data and content data"* has, under Article 8, simply been deferred until 1 January 2008 when:

"The Council shall thereafter review the list of data to be retained in particular with reference to the possibility of including additional types of Internet data."

A clear distinction between access to traffic data and its content is thus blurred.

A further document, 24.10.05, shows the Council working on two tracks: 1) to try and finally agree their own proposal and 2) proposing amendments to the Commission draft Directive: **13624/05**

The big issue, which has obscured the debate over the substantive issues, is the legal basis of the Council proposal. Both the Legal Services of the Council and the European Commission said that the proposal had to be split in two - the mandatory retention of data by service providers coming under the TEC (Treaty establishing the European Communities) where the European Parliament has powers of co-decision (ie: the Council and parliament have to agree on the final text) and access to the retained data by LEAs as a Framework Decision under the TEU (where the parliament is only consulted). See: **Statewatch report and the Opinions of the Legal Services**. Both concluded that if the Council were to pursue a single measure it would almost certainly be challengeable in the Court of Justice. Indeed the Council itself notes if adopted as a single measure it could:

"be annulled: this could result in claims for compensation from any operator who had already been obliged to implement the measure" (EU doc no: 13036/05)

Although these Opinions were dated 22 March 2005 (Commission) and 5 April 2005 (Council) the Council carried on for five months as if they did not exist - only belatedly has the Council grudgingly suggested that it might agree to back the Commission's draft Directive on mandatory data retention, but only if agreement can be reached with the European Parliament by the beginning of December (in time for the Justice and Home Affairs Council on 1-2 December), see, letter from UK Home Secretary, Charles Clarke, representing the UK Council Presidency: **Clarke letter to Cavada** (Mr Cavada is chair of the parliament's Committee on Civil Liberties).

The latest Council document (**13789/05**, dated 28.10.05) sets out:

a. Outstanding issues to be agreed by member states
b. The Council's proposed amendments to the Commission's draft Directive
c. The latest version of the Council's draft Framework Decision (to be read in conjunction with: **12894/1/05)**

What is quite extraordinary about the Council's demand that the European Parliament rush the meaure is that the Council has not even agreed its own final text.

2. The European Commission

The Commission placed on record its reservation about the legal basis of the Council's proposal in autumn 2004. Once the legal opinions of both institutions were published it was only a matter of time before the Commission put forward its own proposal, which it did on 21 September 2005: **Commission proposal for a Directive** and **Commission Extended Impact Assessment**

The Commission's proposal differs from that of the Council in terms of scope. While the Council's proposal covers:

"the purpose of investigation, detection and prosecution of criminal offences.

the Commission says it should cover:

"the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime."

The scope of the Commission's definition is more limited but as "serious criminal offences" are today defined by the EU very broadly it is a major extension from covering terrorism and directly related offences.

What is worthy of note is that the powers under the UK's Anti-Terrorism, Crime and Security Act, passed in 2001, the scope of the retention of data by service and network providers is strictly limied to "national security" and offences "directly or indirectly related to it. Under the Act the Home Secretary can request the retention of data:

"(a) for the purpose of safeguarding national security: or
(b) for the purpose of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security" (Section 102.3, emphasis added)

The Commission's proposal is also:

" far more invasive than the Council proposal. The Commission defines 'communication' as involving "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service". Therefore the Commission is proposing the tracing of all forms of Internet transactions. This means that communications service providers could be compelled to store their mail server logs, web cache logs, and IP flow logs[4] for six months without any regard to necessity or proportionality." (NGO letter to MEPs, 26.9.05)

The Commission's proposal utterly fails to deal with data protection. As its proposal comes under the "first pillar" (TEC) the personal data retained by service and network providers comes under the 1995 Data Protection Directive. Its Extended Impact Assessment simply asserts that as the 1995 Directive has been implemented by all member states there is no need for any further provisions and that "citizens can exercise their powers as granted under these instruments" (p20). But what are the powers of the citizens at national level? Do the powers and resources vary from state to state?

Well the conclusion of the only report on the operation of the 1995 Directive in the member states was published in 2003: **1st report on the 1995 Directive** and its **Technical report** The first report notes that there were variations in powers between states, many data protection authorities were under-resourced and patchy compliance by data controllers. It concludes that if these tendencies are confirmed:

"they are reasons for serious concern and reflections need to be undertaken between the Commission and the Member States and the supervisory authorities to determine their causes and design feasible solutions."

In particular the report notes that:

"The provisions containing safeguards have not been adopted by all Member States. Where they exist, they are often unsatisfactory. The situation is similar as regards Article 8 (4) and (5) - the processing of sensitive data for reasons of public interest or with regard to criminal convictions. The absence of safeguards means the required level of protection for individuals is not being met, which should be a matter of concern for the Member States, as it is for the Commission." (emphasis added)

Whereas the justification for the Commission's proposal on mandatory data retention is to get rid of a "patchwork" of different powers in member states, when it comes to data protection there is silence. The 1995 Directive was implemented in the then members states by 1998 since when there has been just one report whose reservations has also been meet with an institutional silence. Moreover, with the shift of responsibility for data protection from the Internal Market DG to the so-called "Freedom, Justice and Security" DG there is little prospect of any action, see: **Data protection handed to the DG for "law, order and security"**

As noted above the Council's proposal covers two areas: 1) the mandatory retention of telecommunications data by service and network providers - to which the Commission has responded with a proposed Directive and 2) access to the retained data by law enforcement agencies and the exchange of that data between them (and under the "principle of availability" to non-EU states too) - however, **the Commission has yet to published a proposal for a Framework Decision on this second aspect. It is hard to see how the European Parliament can properly consider the first proposal without having sight of, and time to consider, the second one.**

3. EU data protection authorities

The European Data Protection Supervisor (EDPS) has produced a report on the Commission's proposal calling for substantial changes: **EDPS Report**

The Article 29 Data Protection Working Party on the Council initiative by four members states - the Council proposal in November 2004: **Article 29 Working Party opinion** The the Working Party has adopted a further report on the Commission's proposal: **WP 113** (21 October). See also: **Privacy International comments**

The European Parliament should seeks to effect all the recommended amendments proposed by these two bodies.

4. The European Parliament

The first battle for the European Parliament was to insist that the Council proposal be dropped - due to its faulty legal basis - and for two proposals to be presented. One based on the mandatory retention of data under the TEC, on which it has powers of co-decision, and another on access to the data and its transfer under the TEU on which it is only consulted.

A report adopted by the parliament's **Data retention** by Mr Alvaro the rapporteur from the Committee on Civil Liberties sought to clear up the legal basis. Mr Alvaro has since prepared: **Amendments to the Commission proposed Directive** (19.10.05)

European Digital Rights (EDRI) report that Charles Clarke was not at his most diplomatic when he addressed the Committee on Civil Liberties on 13 October. He told the Committee that if they did not agree the proposal before December Justice and Home Affairs Council (1-2 December) the Council would adopted their draft Framework Decision. Moreover he is reported to have told MEPs that if parliament failed to do this "he would make sure the European Parliament would no longer have a say on any justice and home affairs matter".

As is clear from the **Clarke letter to Cavada** (UK Home Secretary, Charles Clarke, representing the UK Council Presidency and Mr Cavada is chair of the parliament's Committee on Civil Liberties) the Council is trying to blackmail the European Parliament with the threat that it will go ahead with its own Framework Decision. In his letter to Mr Cavada, Clarke says:

"the Framework Decision will remain on the table, as an option favoured by a large number of delegations. However, a majority of delegations were also open to a Directive"

The Council is saying if the Directive can be adopted *"by the end of the year"* and the text matches their demands then they will go down this path. *In truth the Council has no choice but to drop its proposal and go along with two draft measures and it knows it.*

Clarke's letter to 17 October is slightly more conciliatory but contains the same veiled threat of reverting to the original Council proposal. He wants to work closely with the parliament "to maximise common ground... by the end of the year". He ends by saying that if all three institutions (Council, Commission and European Parliament) cooperate it will:

"show that we are serious about working together to make a difference to the daily lives of our citizens"

A statement that is ambiguous to say the least - the measure will certainly make a difference, the question is what kind of difference?

At the meeting in the European Parliament of the "Conference of Presidents" (the Group leaders of the parties) on 20 October mandated Mr Cavada and the committee to pursue negotiations with the Council. Such "trilogue" meetings between the Council, Commission and European Parliament representatives take place behind closed doors.

The only way the parliament can meet Charles Clarke's early December deadline is through a first reading co-decision "deal" - by agreeing a set of common amendments to the Commission draft Directive which are then formally adopted by the Council and by the Committee on Civil Liberties and then plenary session of the parliament - this "fast-track" procedure is intended to deal with uncontroversial measures, which is certainly not true in this case.

It should be remember that the need for this proposal was agreed by the Council over four

years ago (20 September 2001) so it is to be hoped that the parliament will not succumb to "inter-institutional" pressure and take all the time necessary to ensure that the liberties and privacy of the people of Europe are properly protected.

5. Civil society

Civil society - NGOs and groups working on civil liberties, privacy, lawyers and journalists - have opposed the measure from the start. They remain unconvinced as to the need and are equally certain that if introduced the powers will, on occasion, be misused and abused. They are not convinced that EU data protection provisions will give any meaningful protection to the individual, who will have no right to be told they have been under surveillance - unless, of course, they are arrested and charged. And if they have no "right to know" they will have no right to correct the data or to be told which agencies information on them has been passed and how it has been added to (inside and outside the EU).

These views are exacerbated by the so-called "principle of availability", invented under the Hague Programme, where intelligence and information held by an agency in one member state can be passed to that in another or to a non-EU state.

Where governments, officials and many parliamentarians are inclined to place their trust in the law enforcement (and security) agencies, concerned civil society see this measure as one of many where these agencies will become self-regulating and unaccountable.

In September 2004 an Open Letter opposing mandatory data retention was sent to the European Parliament from 170 groups/companies - 90 NGOs and 80 telecoms companies: **Open letter on mandatory data retention**

Among the main concerns are:

1. If the security and intelligence agencies - who are at the forefront in stopping terrorist attacks - need access to the telecommunications data to be retained it is very hard to believe that EU governments would have taken over four years to come up with a proposal which will not come into effect for at least two further years. If this is the case they would be guilty of gross negligence and failure to protect the people of Europe. However, if additional powers are needed they should be limited to dealing with terrorism and related offences.

2. The terrible terrorist attacks in the USA, Madrid and London should not be used to justify placing all communications in the EU under surveillance, making everyone a potential "suspect". This is exactly what the EU governments (the Council) want to do when they propose that the retained data can be used for any suspected criminal offence, however minor.

3. The wholesale retention of all communications of everyone is contrary to the findings of the European Court of Human Rights (under Article 8). This interference with the privacy

rights of every user of European-based communications services cannot be justified under the limited exceptions envisaged by Article 8 because it is neither consistent with the rule of law nor necessary in a democratic society. The indiscriminate collection of traffic data offends a core principle of the rule of law: that citizens should have notice of the circumstances in which the State may conduct surveillance, so that they can regulate their behaviour to avoid unwanted intrusions. Moreover, the data retention requirement would be so extensive as to be out of all proportion to the law enforcement objectives served.

4. The question of cost has been fudged by the Council and the Commission. *What has not been highlighted is that service and network providers will be asked to retain a lot more data on each communication than they ever did for billing purpose.* The "institutional consensus" seems to be to leave it to national decision-making whether government are going to help pay for the storage and access to mountains of data or whether the cost will be passed on to the customer. Either way we will all end up paying for our own surveillance.

5. Even the USA has not proposed such a measure, nor will it apply to a service providers from outside the EU.

6. The bottom line is, what kind of society do we want to live in - one where democratic values and standards are maintained in the face in terrorist attacks or one which no Western country would have dared bring about during the Cold War?

"Therefore the European Parliament now faces a crucial decision. Is this the type of society we would like to live in? A society where all our actions are recorded, all of our interactions may be mapped, treating the use of communications infrastructures as criminal activity; just in case that it may be of use at some point in the future by countless agencies in innumerable countries around the world with minimal oversight and even weaker safeguards." (NGO letter to MEPs,2.9.05)

Tony Bunyan, Statewatch editor, comments:

"The Council has failed to convince many of us of the need for this measure. But it is good that on such a momentus issue - placing all the communications of everyone under surveillance - that the European Parliament has the full powers of co-decision. These are powers it should use to the full:

1. The initiative for this measure came out of the EU's reaction to 11 September 2001, its scope should thus be limited to terrorism and directly related offences. If the security and intelligence agencies - who are at the forefront in stopping terrorist attacks - need access to the telecommunications data to be retained it is very hard to believe that EU governments would have taken over four years to come up with a proposal which will not come into effect for at least two further years. If this is the case they would be guilty of gross negligence and failure to protect the people of Europe.

2. To call on the Commission to prepare a report on data protection laws and practices in all member states - the Commission says in its proposal that nothing more is needed on data

protection as this is catered for in national laws, but what protection do these laws provide and do they vary?

3. To introduce amendments to put in place all the recommendations from the European Data Protection Supervisor and the Article 29 Working Party on data protection

4. To review the critiques of NGOs and groups in civil society

The Council has taken four years to bring forward this proposal and still does not have its own agreed text. The European Parliament should take all the time it needs to properly consider the measure for this is what the people of Europe expect - to ensure that these powers are strictly limited in scope and that their rights to data protection and privacy are not endangered."

1. **Civil society letter to Members of the European Parliament on data retention proposals**, from 21 NGOs
2. **Open letter on mandatory data retention** with 170 signatories - 90 NGOs and 80 from industry, September 2004
3. **Privacy International**
4. EDRI: **European Digital Rights**
5. **Quintessenz**
6. **The Register**
7. **Data retention is no solution - petition** signed by 54,998 individuals and 79 organisations
8. **Statewatch database search for "data retention"**
9. International Campaign Against Mass Surveillance (ICAMS) **Report**
10. **Dutch ISPs letter to the European Commission** (pdf)
11. **The Information Technology Association of America (ITAA) comments on proposal** (pdf)

for the general context see:

11. **While Europe sleeps - under the "war on terrorism" a veneer of democracy is legitimating the creation of a coercive (and surveillance) state**
12. **There is no “balance” between security and civil liberties – just less of each**

Filed 01.11.05
