Statewatch report on EU telecommunications surveillance

# Data protection or data retention in the EU?

**- EU governments backing demands of law enforcement agencies**

**- EU governments on a collision course with the European Parliament**

## Introduction - this report describes the situation before the proposals put forward by EU governments on 20 September 2000

The debate over the demands of the EU law enforcement agencies that telecommunications traffic and location data be retained, and that they should have access to it, is reaching a crucial stage. At present under existing EU Directives this data has to be erased or made anonymous and such data can only be kept for billing purposes (ie: to aid the customer).

The fight is centred on a new draft Directive on "the processing of personal data and the protection of privacy in the electronic telecommunications sector" which would update the existing 1997 Directive on this issue. The Commission's draft proposal simply updates the provisions to cover new means of communication (eg: the internet and e-mail).

The European Parliament report from the Committee on Citizens' Freedoms and Rights came out strongly in favour of the existing Directives and against data retention. The Council of the European Union (the 15 EU governments) have agreed a position which would allow for data retention and its surveillance by law enforcement agencies.

The report from the Committee on Citizens' Freedoms and Rights (LIBE) on the proposed new Directive was rejected by plenary session of the European Parliament on 5 September by 204 votes to 129 with 155 abstentions (the primary reason for the report's rejection was the issue of "spam", unsolicited e-mails). This special report by Statewatch looks at the latest developments on proposals to place telecommunications under surveillance. As the EU's Data Protection officials observe, the outcome will fundamentally affect the future of democracy in the EU. If the parliament's report is adopted unamended and the Council then adopts its opposing common position the two institutions will be on a collision course.

## "ENFOPOL 98" agreed, Conclusions on hold

The meeting of the EU Justice and Home Affairs Council on 28-29 May agreed a "Council Resolution on law enforcement operational needs with respect to public telecommunications" which effectively adopts the extension of surveillance in "ENFOPOL 98" (see Statewatch, vol 7 no 1 & 4 & 5; vol 8 no 5 & 6; vol 10 no 6; vol 11 no 1 & 2; the final legislative text is in ENFOPOL 55, 20.6.01). Its formal adoption has been delayed due to a scrutiny reservation by Germany - when this is withdrawn it will be nodded through.
The Resolution defines how the "Requirements" to be placed on network and service providers are to be interpreted in the EU (see Statewatch vol 11 no 2 for details of its effect). The "Requirements" were adopted by the EU on 17 January 1995 and mirrored those drafted by the FBI in the USA.

The draft Council "Conclusions" in ENFOPOL 23 (30.3.01) which seeks to make an overall statement on the demands of the EU law enforcement agencies for the retention and access to all traffic data. They also call on the Commission to review all existing EU laws which effect

this surveillance. The proposal is currently on hold because some member states do not think it appropriate for a "third pillar" (justice and home affairs) initiative to law down the law to the Commission and the Telecommunications Council ("first pillar", economic and social policy).
Statewatch's application to the Council for a copy of ENFOPOL 23 + COR 1 (which makes clear this is a proposal from both the Swedish and French delegations), was discussed at two meetings of the Working Party on Information. The first meeting concluded that: "the applicant may have access to the documents requested (provided that the French and Swedish delegations agree)." However, on 23 May it was decided that:

"The document was agreed to be withheld because the French delegation so wished"
The text of ENFOPOL 23 is on the Statewatch website: www.statewatch.org/soseurope.htm

## Divisions in the Council and adoption of "guidelines"

Since last autumn when the discussions on the new Directive in the Council on the needs of the law enforcement agencies (LEAs) to have access to telecommunications data came back onto the agenda there were divisions amongst the member states (see Statewatch vol 11 no 2). Belgium, Germany, France, Netherlands, Spain and the UK wanted to delete the requirement that traffic data must be erased or made anonymous in the 1997 Directive and the LEAs given access to the data.

On 29 May the Telecommunications Working Party discussed the Council's draft position. Three delegations, Sweden (the then Presidency of the EU) and Belgium (the next Presidency) and the United Kingdom wanted to delete from Article 6.1. the requirement to erase data or make it anonymous because it:

> *"does not take into account the needs of the repressive agencies"*

Greece, Italy and the Netherlands, together with the Commission, refused:

> *"to see the text of the present directive changed on this point and insisted on the importance and sensitivity of this issue which affects human rights and fundamental rights"*

The UK also argued in favour of changing Article 15 to allow general retention of data and the Swedish Presidency proposed that the following was added to Article 15.1:

> *"Member states may provide for the retention of data for a limited period.."*

The final version sent by the working party to COREPER (the permanent committee of top-level representatives from the 15 EU governments based in Brussels) included a wording put forward by Belgium (the incoming EU Presidency). This proposed removing the requirement in Article 6.1. to delete traffic data and inserting that the data could be:

> *"processed for legitimate purposes as determined by national law or applicable instruments" (29 May)*

At the meeting of COREPER on 13 June the UK tried to insert an enabling clause for law enforcement purposes in Article 15.1.

The wording of Article 15.1. allows member states to derogate from the Directive for the purposes, among others, of national security and the prevention, investigation, detection and prosecution of crime. Indeed there is nothing in the present or proposed Directive preventing EU member states, on an individual basis, from adopting national laws allowing for the general retention of data for law enforcement purposes. However, such measures would have to be compatible with community law especially Article 8.2 of the European Convention on Human Rights and the consequent case law in the European Court of Justice.
However, the demands of the law enforcement agencies, backed by a number of powerful

governments, require that all EU states (and thus all applicant states) be bound to adopting the same powers of surveillance. The argument is that there cannot be a situation where country A allows data retention but country B does not.

The "informal" text of the Council's position was agreed at the Telecommunications Council on 27 June - this text is termed "guidelines" rather than the Council common position as the European Parliament has not yet adopted its first reading position.

The amended text sent from COREPER to the Telecommunications Council inserted at the end of Article 15.1. a new sentence saying that in derogating from the Directives provisions EU governments "may provide for the retention of data for a limited period". In order to get unanimity this was deleted at the Council and a revised "Recital 10" was agreed saying:

> *"this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications or take other measures, such as providing for the retention of traffic or location data for a limited period, where necessary and justified for these purposes"*

The purposes are as set out in the existing Directive "to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences". However, most existing national interception laws only covers those authorised on an individual basis for a specific suspected offence - not the general retention of data for law enforcement purposes. Although the Council is now not proposing a change to the main text of the new Directive the change to this Recital will, in their view, give a green light for EU governments to adopt new laws at national level ending the erasure of data, requiring data to be retained, and for law enforcement agencies to have access to this data. The effect would be to fatally undermine data protection and privacy in the EU.

## EU data protection letter

In the midst of these discussions Stefano Rodotà, chair, of the EU's Data Protection Working Party sent a letter to the European Parliament, the European Commission and the Council. The letter is blunt calling on them to back the Commission's initial proposal:

> *"It seems that some Member States would like to change the balance in favour of increasing the possibilities of law enforcement authorities beyond the scope of what the European Court on Human Rights has accepted in the course of its case law on Article 8 of the European Convention of Human Rights.*
>
> *The Article 29 Data Protection Working Party considers that the Council and the European Parliament should resist any changes of the existing provisions guaranteeing confidentiality of communications (Article 5) and limited processing of traffic data (Article 6). It is not acceptable that the scope of initial data processing is widened in order to increase the amount of data available for law enforcement objectives. Any such changes in these essential provisions that are directly related to fundamental human rights, would turn the exception into a new rule. Systematic and preventive storage of EU's citizens' communications and related traffic data would undermine the fundamental right to privacy, data protection, freedom of expression, liberty and presumption of innocence. Could the Information Society still claim to be a democratic society under such circumstances?"*

## Some EU governments jump the gun

Evidence has emerged that some EU governments have already taken steps to require the retention of data, thus putting pressure on others to do the same. In the Netherlands legislation requires internet service providers to store connection data for three months. Belgian law requires them to keep call data for a minimum of 12 months and France is also preparing a law requiring the retention of connection data for 12 months. While official responses to a survey carried out by the EU's Police Cooperation Working said:

*"the United Kingdom have concluded informal arrangements for national service providers whereby UK investigative departments hope that connection data will be stored for 12 months"*

This admission contradicts statements given by two Ministers - Patricia Hewitt and Charles Clarke - that the government was not planning any measure on data retention. Or rather they said: "We have no plans to introduce legislation mandating the retention of such data" (letter to Sunday Independent, 28.1.01). Instead it appears they have followed the advice of the report from the National Criminal Intelligence Service (see Statewatch, vol 10 no 6) for an "informal" agreement - as legislation going through parliament might be contentious.

The EU report said that all member states wanted telecommunications providers to be obliged "to store connection data for a minimum period... a minimum period of 12 months".

## European Parliament report

On 11 July the European Parliament's Committee on Citizens Freedoms and Rights adopted a report on the new Directive by 22 votes to 12 with 5 abstentions. A mixed alliance: the PPE (conservative group), ELDR (Liberal group), some PSE (Socialist group) and Turco and Cappato (Italian Radicals) voted in favour, the majority of the PSE (Socialist group) voted against with the GUE (United Left) and the Green/EFA groups abstaining.

The critical amendments in the report are to Recital 10 and to Article 15. Article 15 allows member states on an individual basis to restrict the limits of the Directive for national security and the prevention, investigation, detection and prosecution of crime. The parliament's amendment would add the following:

*"These measures must be entirely exceptional, based on a specific law which is comprehensible to the general public and be authorised by the judicial or competent authorities for individual cases. Under the European Convention on Human Rights and pursuant to rulings issued by the Court of Human Rights, any form of wide-scale general or exploratory electronic surveillance is prohibited".*

There was much discussion not around data retention but around unsolicited e-mails and faxes (which the Commission wants to prohibit and criminalise, so do the PSE group). The adopted text in the Cappato report leaves these issues to national decision-making. The draft Council "guidelines" want to extend the ban on unsolicited e-mails to "political campaigns" which would negate NGO/voluntary group work.

On 19 July the Council's Working Party on Telecommunications discussed the parliament's report and concluded that "the possibility of agreement at first reading with the European Parliament was not the likeliest hypothesis". At the Working Party meeting Germany requested that discussion be re-opened on Article 6 (data retention) but this was not accepted by other member states.

## Conclusion

The first draft of the report agreed by the Committee on Freedoms and Rights in effect keeps the position of the 1997 Directive that data can only be kept for billing purposes. Whether this position can be maintained during future discussions remains to be seen. The outcome, as the EU's Data Protection officials observe, will fundamentally affect the future of democracy in the EU.

For sources and full-text documentation see:

**www.statewatch.org/news/2001/may/03Cenfopol.htm**