



Statewatch analysis

Mandatory retention of telecommunications traffic to be "nodded" through in UK

- the EC Directive on mandatory retention will be adopted in the UK without any meaningful debate by simple "affirmative" votes in parliament
- the government is saying that the EC Directive covering serious crime can be used for *any* crime however minor
- the government is saying that there is no need for public or parliamentary discussion on privacy, civil liberties or human rights issues as these have already been discussed at the EU level
- the annual report of the Interception of Communications Commissioner says there were a staggering 439,054 requests to service providers for communication data by the law enforcement agencies

Introduction

The UK government is intending that the mandatory retention of communications data by telephone service providers (all phone-calls, faxes, mobile phone-calls and locations) be introduced by a Regulation. The procedure for the adoption of a "Regulation" is simply that the measure is "laid" before parliament and passed by an "affirmative vote" in the Commons and Lords - unless a large number of MPs and/or peers insist on a debate there will not be one.[¹]

Later, by March 2009, the retention of communications data on all internet usage (sites visited, internet e-mails and telephony via net) will be mandatory.

The measure will put into UK law the highly-contentious EC Directive on mandatory data retention adopted in 2005 and will replace the current "voluntary" Code introduced in the UK in 2003.[²]

¹ It is due to come into effect by 15 September 2007.

² See Statewatch Observatory: The surveillance of telecommunications in the EU: <http://www.statewatch.org/eu-data-retention.htm>

Under the Anti-Terrorism, Crime and Security Act (ATCSA) 2001 service providers can *collect* and *retain* traffic data for the limited purpose of "national security" (and related criminal offences). On the other hand, the "voluntary" Code allowed the data collected and retained to be accessed and used by law enforcement agencies for *all* crimes, however minor, under the Regulation of Investigatory Powers Act 2000 (RIPA)³. This situation led some providers not joining the voluntary Code due to the ambiguous legal position, although the "majority" of service providers were happy to take part in the voluntary code and proactively "assist law enforcement and intelligence agencies"(p5). The paper recognises the problem as:

"the disparity that can exist between purposes for which data may be lawfully retained and lawfully obtained"(p4)

This problem is compounded by the scope of the EC Directive on mandatory data retention is limited to the:

"investigation, detection and prosecution of serious crime" (emphasis added)

"Serious crime" is clearly wider in scope than "national security" (and related offences) but it does not legitimise the use and exchange of the data collected for all crime however minor.

The consultation paper

The Consultation paper (full-text including the EC Directive and the draft Regulation, see Sources) was put out on 28 March 2007.

None of the seven questions posed in the paper deal with privacy or data protection as the paper says these issues were dealt with when the voluntary Code was out for consultation back in 2003 and that "human rights considerations" were dealt with in the:

"debate about the Directive in the European Council and the European Parliament" (Human Rights considerations, p6)

In the European Parliament the two big parties steam-rolled the Directive through against highly vocal opposition from data protection authorities and civil society groups.

The argument that debate is unnecessary, apart from being highly questionable, does not hold water since transposition of the Directive would replace a voluntary code by a binding law. In such circumstances a full debate

³ Chapter II of Part I, Section 22.2 of RIPA says communications data can be accessed and used in relation to "crime", that is all crime.

is required.

Along with most other EU governments the UK is putting off the date for traffic data "relating to internet access, internet telephony and internet e-mail" until 15 March 2009 - because this is more "complex an issue involving much larger volumes of data"(p5).

As to the need for the Regulation the paper says:

"The Directive rightly references terrorist atrocities in Madrid and London in making the case for adopting measures for retention of communications data across Europe"

But the Regulation does not just cover terrorism, but all crime however minor.

The paper leaves service providers with a wide power to hold traffic data for longer than the 12 months set out in the Regulation:

"The proposed Regulation will not prevent businesses from keeping data for longer than our proposed retention period..."(p4)

But how would such longer periods of data retention by service providers be legally justified? They can only be justified according to Article 13(1) of Directive 2002/58 - and there is very little scope there to give the service providers power to keep the data for longer than necessary for service provision, etc. unless the government has ordered them to do so on security grounds. Technically it is true to say that the Regulation transposing the data retention Directive would not stand in the way of longer periods of data retention by service providers, but it is hugely misleading not to mention that the earlier Directive would stand in the way of this.

In support of its argument for data retention the paper cites a "two week survey" by ACPO (Association of Chief Police Officers) with headline figures concerning 231 requests for data of which 60% concerned murder and terrorism.

However, the figures published in the annual report from the Interception of Communications Commissioner, published in February 2007, said that there were a staggering 439,054 requests lodged for communications data. The Commissioner comments that it is the law enforcement agencies:

"who are the principal users of communications data [who] have acquired fully automated systems" (emphasis added)

The proposal to transpose the Directive into a Regulation

The consultation paper notes that Ireland and Slovakia are challenging the legal basis of the Directive in the European Court of Justice and then says (point 6.5):

Statewatch analysis - Mandatory data retention in the UK / 3

"Regulations passed by parliament under the European Communities Act 1972 will be unaffected if the Directive is subsequently annulled"

This assertion is clearly wrong legally - Regulations passed under the European Communities Act (ECA) would be undoubtedly invalid if the Directive is annulled - that is the whole point of a number of judicial review proceedings against ECA Regulations or intended ECA Regulations that have been brought in the past (ie: the argument is that the ECA Regulations are invalid precisely because the Directive is invalid).

This would be true if the Directive were annulled on any ground - and in particular if it were annulled for the reasons that the Irish and Slovaks argue, that the EC has no power at all to adopt the Directive. If that is correct, then the ECA could not possibly be used to implement the "Directive", since the ECA only gives the UK government the power to implement Community measures (ie first pillar measures) by Statutory Instruments.

Although the government intends to put off until March 2009 the mandatory retention of data from the internet (internet access, e-mail and telephony) they intend to continue with the "voluntary arrangements" in operation at present - in other words the majority of service providers are already making this data available.⁴

Thus nothing in the Regulation to transpose Article 1.1. of the EC Directive, ie: the limitation of use of the data to investigate, etc. serious crimes as defined by national law.

As a matter of human rights/data protection law the circumstances in which the data will be processed must be foreseeable in legislation, otherwise the interference with private life is not "prescribed by law" as ruled by the courts.

Also there is nothing in the Regulation transposing Article 13 of the Directive, covering sanctions and remedies relating to unauthorised use of the data, etc. It may be that there is adequate provision in the Data Protection Act and/or other Regulations transposing EC data protection legislation but this should have been explained at least in the impact assessment and summary and referred to in the Regulation itself. There is an obligation when transposing directives to make a clear reference to the national legal rules which transpose the directive so that individuals can identify their rights - arguably since there is not even a cross-reference in this draft Regulation to the rules elsewhere which transpose Art 13 already (assuming there are such rules) this obligation has not been met.

Nor is there any reference to the transfer of communications data to other EU

⁴ For this reason they intend to extend the deadline in the "sunset clause" in Section 106 of the ATCS Act 2001.

states or to third countries - which would have to be covered by a “third pillar” measure.

Tony Bunyan, *Statewatch* editor, comments:

“The collection and retention of everyone’s communications data is a momentous decision, one that should not be slipped through parliament without anyone noticing as the government plans to do.

The government’s proposal changes a voluntary agreement into a binding law, on these grounds alone there should be primary legislation.

Moreover, the EC Directive limits the purpose for which data can be retained to “serious crime” but the government intends to extend the scope to all crime however minor.

Sources (click for access)

The Home Office Consultation paper on mandatory data retention of telecommunications (full-text, pdf):

<http://www.statewatch.org/news/2007/mar/uk-ho-cons-eur-dir-data-ret.pdf>

EC Directive on mandatory data retention 2003:

<http://www.statewatch.org/news/2007/mar/uk-ec-reg-2003.pdf>

UK: Data retention and access consultation farce

<http://www.statewatch.org/news/2007/mar/uk-ho-cons-2003-data-ret.pdf>

Statewatch report and the Opinions of the Legal Services - which led to the legal basis of the proposal to be changed:

<http://www.statewatch.org/news/2005/apr/02eu-data-retention.htm>

Data retention and police access in the UK - a warning for Europe:

<http://www.statewatch.org/news/2005/nov/01uk-eu-police-access-to-data.htm>

Open letter from civil society to the European Parliament:

<http://www.statewatch.org/news/2004/sep/data-retention.htm>

"The European Parliament and data retention: Chronicle of a 'sell-out' foretold?": http://www.statewatch.org/news/2005/dec/sp_dataret_dec05.pdf

Statewatch Observatory: The surveillance of telecommunications in the EU:

<http://www.statewatch.org/eu-data-retention.htm>

May 2007