Analysis

Mass surveillance of communications in the EU: CJEU judgment and DRIPA 2014/RIPA 2000 in the UK

Tony Bunyan
(August 2014)

- **UK ignores EU court judgment that the EU Data Retention Directive is unlawful**
- **No change to GCHQ "spying on the rest of the world"**

- **Mass surveillance of communications means the: *"private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.... It therefore entails an interference with the fundamental rights of practically the entire European population." (CJEU)***

On 8 April 2014 the Court of Justice of the European Union (CJEU) found the the 2006 EU Directive on mandatory data retention was unlawful [1] and had been so since the day it was passed. The judgment followed a critical Opinion of the Court's Advocate-General delivered on 12 December 2013. [2]

The CJEU judgment is damning in its rejection of mass surveillance based on the retention of data on every communication by everyone resident in the whole EU. The judgment (emphasis added throughout) says that the data:

> *"taken as a whole, may allow very precise conclusions to be drawn concerning the **private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.**"* (para 27)

And:

> *"the fact that data are retained and subsequently used without the subscriber or registered user being informed is **likely to generate in the minds of the persons***

[1] http://www.statewatch.org/news/2014/apr/eu-ecj-data-ret-judgment.pdf

[2] http://www.statewatch.org/news/2013/dec/eu-ecj-advocate-general-opinion-data-retention-C-293-12.pdf

> ***concerned the feeling that their private lives are the subject of constant surveillance****."* (para 37)

Everyone is a suspect as it:

> *"applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users.* ***It therefore entails an interference with the fundamental rights of practically the entire European population****."* (para 56)

Innocent people are caught up in the web of "suspicion"

> *"Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services,* ***but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.*** *Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy."* (para 58)

On the passing of personal data outside the EU (e.g. to the USA):

> *"[The] directive does not require the data in question to* ***be retained within the European Union****, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security."* (para 68)

The CJEU concludes:

> *"Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has* ***exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.****"* (para 69).

The Court considered in depth the powers of the powers of national states' to require CSPs/ISPs to retain data for law enforcement purposes under EU Directive 2002/58 [3]. This Directive does allow data to be held by providers for the purpose of billing and the provision of the service. However, this covers a very limited period (a few days in many casas) and as the Advocate-General notes the Data Retention Directive "derogates from the system of protection of the right to privacy as established by Directives 95/46 and 2002/58.[4] This is why the Court concluded that "amending Directive 2002/58" was also invalid.

Already a legal challenge has been launched against the DRIPA Act 2014 in the UK, see below [5], a challenge has been launched in Switzerland [6] and in Slovenia the Constitutional

---

3 http://www.statewatch.org/news/2014/aug/eu-dir-privacy-2002-58.pdf

4 Judgment para 32.

5 http://www.out-law.com/en/articles/2014/july/legal-challenge-lodged-against-new-uk-data-retention-laws/

Court has ruled data retention to be unconstitutional [7] and ordered deletion of data collected under the law [8]

Three months after the judgment was handed down the UK government announced it would push emergency legislation through parliament "to ensure police and security services can continue to access phone and internet records". [9] Steve Peers, Professor of Law at the University of Essex subsequently observed that:

> *"the government's intention, as manifested by the Bill, to reinstitute mass surveillance of telecoms traffic data is a clear breach of the EU Charter of Fundamental Rights."* [10]

On the over-arching issue of requiring the mass surveillance of all forms of communication Peers says:

> "*if the broader interpretation of the Court's judgment is correct: no mass surveillance is possible. If that is correct, then the provision in the draft Bill to permit a requirement to collect 'all' data is inherently suspect, and it would certainly be a breach of EU law to require telecom providers to retain all traffic data within the scope of the e-privacy Directive without some form of further targeting"*

UK: Data Retention and Investigatory Powers Act 2014 [11]

Criticism of the Bill came from all quarters, but the Data Retention and Investigatory Powers Act 2014 (DRIPA) nevertheless passed through the UK parliament in just three days, amending the Regulation of Investigatory Powers Act 2000 (RIPA). [12] The DRIPA Bill was accompanied by an Explanatory Memorandum, Impact Assessment and Data Retention Regulations 2014 [13]. The crucial "Code of Practice", which should include safeguards for professional secrecy (e.g. for lawyers, journalists, etc.) has yet to be published. See: Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN briefing on the fast-track Data Retention and Investigatory Powers Bill (pdf). [14]

---

6 http://sustainability.oriented.systems/challenging-swiss-data-retention/

7 https://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=1256&cHash=2885f4a56e6ff9d8abc6f94da098f461

8 http://www.digitalrights.ie/data-retention-slovenia-unconstitutional/

9 'Emergency phone and internet data laws to be passed', *BBC News*, 10 July 2014, http://www.bbc.co.uk/news/uk-politics-28237111

10 http://eulawanalysis.blogspot.co.uk/2014/07/does-uks-new-data-retention-bill.html

11 http://www.statewatch.org/news/2014/jul/uk-drip-act-2014.pdf

12 http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf

13 http://www.statewatch.org/news/2014/aug/uk-dripa-reg.pdf

14 Data Retention and Investigatory Powers Act 2014: http:/www.statewatch.org/news/2014/jul/uk-drip-act-2014.pdf; Regulation of Investigatory Powers Act 2000: http:/www.statewatch.org/news/2014/jul/x-ripa-2000.pdf; Explanatory Memorandum: http:/www.statewatch.org/news/2014/jul/uk-bill-data-ret-em.pdf; Impact Assessment: http:/www.statewatch.org/news/2014/jul/uk-drip-ia.pdf; Draft Regulation: ; Data Retention Regulations 2014: http://www.legislation.gov.uk/uksi/2014/2042/pdfs/uksi_20142042_en.pdf Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN Briefing:: http://www.statewatch.org/news/2014/jul/uk-briefing-on-the-Data-Retention-and-Investigatory-Powers-Bill.pdf

The Regulation says that the details required to issue a warrant under S5.b should now include: "the likely number of users (if known)". This relates to the fact that a warrant can be against a "person", defined in RIPA 2000 as: "any organisation or any association or any combination of persons". Thus a warrant against a "person" could cover the headquarters of the National Union of Journalists HQ or the Trades Union Congress. The term "if known" is worrying and the test will be if these figures are made public.

Section 10 of the Regulation makes provision for a statutory Code of Practice on the retention of data but it is noteworthy that this code **will not**:

> *"include a reference to any such powers and duties which are conferred on the Secretary of State."* (cf. S.71, RIPA 2000)

These powers and duties include, for example, the Secretary of State (the Foreign Secretary in the case of GCHQ) signing an unlimited and open-ended warrant-certificate under Section 8.4 of RIPA 2000 to "spy on the rest of the world".

Section 14 of the Regulation revokes the 2009 Regulation (itself preceded by the 2007 Regulation) which brought the UK in line with the EU Data Retention Directive and "provides for transitional arrangements for data retained under those regulations".[15]

UK by-passes the EU to protect its global surveillance regime

The UK failed to notify the European Commission of its intention to introduce a new Act revoking the 2009 Regulation until after it was passed. A number of NGOs raised the issue in an Open Letter to Vice-President Michel Barnier and Commissioner Cecilia Malmstrom::

> *"We, the undersigned organisations, would like to draw your attention to an infringement of EU law by the United Kingdom through its adoption on July 17 2014 of the Data Retention and Investigatory Powers Bill ("DRIP")".*[16]

This drew the following comment:

> "*For the British journalist Liat Clark, this law is a "finger salute to Europe." The old law, dating from 2006, was made inapplicable by the Court of Justice of the European Union (CJEU) in April, and found to be unlawful, particularly because of its overly broad spectrum."* [17]

The UK is the first EU government to change its law on data retention following the Court of Justice of the European Union's judgment in April annulling the 2006 Directive. It has not waited for the European Commission to decide whether or not to replace the 2006 Directive.

At the moment the Commission is sitting on the fence by saying it is up to each of the 28 EU states to decide whether to change their national laws in the light of the judgment (see

---

[15] http://www.statewatch.org/news/2014/apr/uk-mand-ret-2009.pdf

[16] http://www.statewatch.org/news/2014/jul/uk-eu-dripa-ngo-letter.pd

[17] http://www.lemonde.fr/pixels/article/2014/07/18/le-royaume-uni-adopte-une-nouvelle-loi-sur-la-surveillance-electronique_4459799_4408996.html

European Parliament Question [18] and Answer [19] which suggests that national data retention regimes can still maintain or set up new data retention schemes, under the conditions of Article 15(1) of the e-privacy Directive (2002/58). But they would have completely re-write current laws (based on the "unlawful" 2006 EU Directive) in full recognition of the strong limits and safeguards in the CJEU's judgment, which expressly excludes the mass surveillance of the whole population and the exchange of personal data with non-EU states.

This fudge could lead to 28 different laws. In Germany, for example, it would be unlawful for a Communications Service Provider (CSP) or Internet Service Provider (ISP) to agree to an order laid on them by the UK government to gather, hold and exchange personal data. It would seem to be only a matter of time before a "harmonising" Directive is back on the table.

"Permanent capability" for CSPs/ISPs to store personal data required

The main amendment introduced by DRIPA 2014 is concerned with issuing warrants to commercial companies outside the UK (i.e. in the EU and the USA). However it should be noted that according to the Explanatory Memorandum accompanying the Bill, the new Sub-Section (3A) specifies (emphasis added):

> *"the Secretary of State's power to give **a notice requiring the maintenance of a permanent capability** to a telecommunications service provider."*

The UK will only issue one notice to companies providing a service to or in the UK. All external service providers will be required to maintain a permanent capability to capture and hold communications data and content for up to 12 months - and allow access to UK law enforcement agencies. The Explanatory Memorandum said this is meant to make explicit what was originally "intended" - which is a pretty weak argument as it is not all evident in RIPA 2000 that this was so.

DRIPA 2014: GCHQ can still "spy on everyone in the world"

DRIPA 2014 leaves in place the Secretary of State's powers under S.8.4 of RIPA 2000 to issue limitless "certificates" which allow it to spy on the rest of the world for example by GCHQ scooping up all the traffic from fibre-optic cables going entering and leaving the UK. [20]

The UK is consciously acting in defiance of the CJEU ruling on mandatory data retention by requiring all CSPs/ISPs inside and outside the UK to permanently store information on all communications they handle - mass surveillance.

Tony Bunyan, Statewatch Director, comments:

> *"The CJEU ruled that mass surveillance under the EU Data Retention Directive entails an interference with the fundamental rights of practically the entire European population and is a clear breach of the EU Charter of Fundamental Rights.*

---

[18] http://www.lemonde.fr/pixels/article/2014/07/18/le-royaume-uni-adopte-une-nouvelle-loi-sur-la-surveillance-electronique_4459799_4408996.html

[19] http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2014-005254&language=EN

[20] http://www.statewatch.org/analyses/no-244-gchq-intercept-commissioner.pdf

"Under DRIPA 2014 the UK is clearly ignoring the Court's ruling by maintaining the mass surveillance of communications and extending its reach, though permanent warrants, to service providers based in the EU, USA and elsewhere.

"DRIPA 2014 amends RIPA 2000 but leaves untouched the power of the Foreign Secretary to sign limitless warrants for GCHQ to spy on the rest of the world under Section 8.4 of RIPA 2000."