No to Bulk Data Retention: The Watson Case in the CJEU

Joined Cases C 203/15 and C 698/15

Tele2 Sverige AB v Post- och telestyrelsen

Secretary of State for the Home Department v Tom Watson MP, Peter Brice and Geoffrey Lewis

Imogen Proud, Monckton Chambers

Days before Christmas, the Court of Justice of the European Union ('CJEU') clarified EU law on the bulk retention by governments of communications data. Communications data does not include the content of a communication but does reveal the other information including the sender, recipient, time, place and method of communication. The Grand Chamber ruled that "general and indiscriminate" retention of electronic communications data for the purpose of fighting crime is unlawful. National legislation is also precluded which governs the protection of and access to stored communications data where (i) the objective pursued is fighting crime but is not restricted solely to fighting *serious* crime, (ii) access is not subject to prior review by a court or independent administrative authority and (iii) there is no requirement that the data be retained within the EU.

The UK Judicial Review

The UK Court of Appeal's request for the preliminary ruling was made in the context of an appeal against judicial review proceedings between Tom Watson MP, Peter Brice and Geoffrey Lewis and the Home Secretary. I have written previously (here) on the Court of Appeal's ruling that the reference to Luxembourg be made.

The judicial review concerned the Data Retention and Investigatory Powers Act 2014 ("DRIPA"), a coalition government piece of emergency legislation, which received royal assent on 17 July 2014. The challenge was originally brought by David Davis, when he was a backbench Conservative MP, and Tom Watson, Labour's deputy leader. David Davis withdrew from the case following his ministerial appointment as Brexit Secretary.

Section 1 of DRIPA empowers the Home Secretary to issue a notice requiring any public telecommunications operator to retain relevant communications data

for up to 12 months. The Home Secretary must consider the requirement to be necessary and proportionate for one or more of the purposes in s22(2)(a)-(h) of the Regulation of Investigatory Powers Act 2000.

These purposes include national security, crime prevention and public safety. There is no requirement in the legislation that the issuing of a retention notice be subject to prior judicial or independent authorisation, nor that the crime in question be *serious* crime.

The Divisional Court ([2015] EWHC 2092 (Admin)) found section 1 of DRIPA to be contrary to the CJEU's earlier judgment in Joined Cases C/293/12 and C/594/12 *Digital Rights Ireland Ltd* and *Seitlinger and Others* ("*Digital Rights Ireland*"). It disapplied section 1 with effect from March 2016. The Home Secretary appealed against the Divisional Court's judgment.

Digital Rights Ireland

The CJEU's judgment of 8 April 2014 in *Digital Rights Ireland* invalidated the Data Retention Directive (2006/24/EC) as it was found to constitute a disproportionate interference with Articles 7 (right to privacy) and 8 (right to protection of personal data) of the EU Charter of Fundamental Rights (the 'Charter'). The CJEU identified safeguards which were absent from the Data Retention Directive including a lack of clear rules governing access to the retained data and specifically the absence of any requirement for prior judicial or independent authorisation for access.

The parties to the judicial review disputed whether the CJEU was only pointing out flaws with the Data Retention Directive or whether it was *additionally* laying down mandatory requirements of EU law which any domestic data retention legislation must meet in order to be lawful. The Divisional Court held the latter, and found that s1 DRIPA did not meet the *Digital Rights Ireland* requirements that (1) communications data be used only for the purpose of combating serious crime and (2) access to data be subject to prior review by a court or independent administrative body. The Court of Appeal accepted, on a provisional basis, the Home Secretary's argument that *Digital Rights Ireland* did not lay down any such mandatory requirements.

At the request of the Home Secretary, the Court of Appeal referred questions to the CJEU concerning the correct interpretation of *Digital Rights Ireland*, in particular whether the judgment lays down mandatory requirements of EU law applicable to a Member State's domestic data retention regime.

Tele 2

The UK's reference was joined with one made by the Swedish Administrative Court. The Swedish reference concerned Swedish legislation requiring communications service providers to retain certain broad categories of communications data for 6 months and providing for its disclosure to national law enforcement bodies. Following *Digital Rights Ireland*, a Swedish provider of electronic communications services had ceased to retain and send to the National Police Authority its electronic communications data, on the basis that obligation to do so was incompatible with the Charter. The Swedish court referred questions concerning the compatibility of a general and indiscriminate obligation to retain communications data with EU law, and particularly with 2002/58/EC (the 'E-Privacy Directive').

The Judgment

The primary question which the CJEU answered was whether the E-Privacy Directive, read in the light of Articles 7 and 8 of the EU Charter, precludes general data retention obligations (such as those found in DRIPA and the Swedish legislation).

The E-Privacy Directive establishes the general 'principle of confidentiality of communications' - that communications data should be erased or made anonymous when no longer required for the transmission of a communication (Article 5(1)). Article 15(1) then introduces a derogation from that general rule permitting Member States, where justified on specified grounds, to restrict that obligation to erase or render anonymous, or even to make provision for the retention of data.

However, the Article 15(1) derogation applies only when "strictly necessary" ([96]), so that the exception is not permitted to "become the rule" ([89]). Article 15(1) expressly provides that the measures which it permits shall be in accordance with the general principles of EU law. As this now includes the fundamental rights now guaranteed by the Charter, the derogation must be interpreted in the light of the Charter, and in particular Articles 7 and 8 ([91]). Any limitation on the exercise of Charter rights must be provided for by law, respect the essence of those rights, and respect the principle of proportionality.

The Grand Chamber reasoned that the bulk retention of communications data constitutes a "particularly serious" interference with Articles 7 and 8 ([100]). National legislation which permits or requires the "general and indiscriminate" retention of all communications data exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) read in the light of the Charter [107]. National data

retention legislation is precluded where its aim is to fight crime, but where this is not limited to *serious* crime [(102)]. It is likewise ruled out where access to the data is not subject to prior review by a court or an independent administrative authority, or where there is no requirement that the data concerned should be retained within the EU [125].

However, Article 15(1) does not prevent a Member State from "adopting legislation permitting, as a preventive measure, the targeted retention of … data, for the purpose of fighting serious crime, provided that the retention of data is limited" [108]. This is provided that the retention is limited to what is strictly necessary, in terms of the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted [108]. In order to satisfy these requirements, the national legislation must:

- lay down clear and precise rules governing the scope and application of data retention and imposing minimum safeguards [(109)];

- in the context of fighting crime:

  (i) ensure the retention of data meets objective criteria that establish a connection between the data to be retained and the objective pursued such as actually to circumscribe the extent of that measure [(110)]; and

  (ii) be based on objective evidence identifying data likely to reveal a link with serious criminal offences [(111)].

Comment

(1) DRIPA contained a sunset clause, which meant the Act expired on 31 December 2016 – just 10 days after this judgment was handed down. This judgment is likely nonetheless to have important domestic ramifications, not least for the Investigatory Powers Act 2016 ('IPA') (branded the 'Snooper's Charter' by its critics) which replaced DRIPA, receiving Royal Assent on 29 November 2016. Section 87 of that Act provides for data retention for the purpose of fighting any crime, whether serious or not. There is no requirement that retention be targeted, nor that there be prior judicial or independent review in most cases.

Liberty, which represented Davis and Watson in their judicial review of DRIPA, has already stated that the Investigatory Powers Bill is 'ripe for challenge' and is currently crowdfunding for this purpose (for example, see here). Whilst the UK remains subject to the CJEU's jurisdiction, this preliminary ruling has made it significantly more likely that such a challenge to IPA on grounds of incompatibility with EU law would succeed. Theresa May, in her speech on

Brexit on 17 January 2017, set out that "*we will take back control of our laws and bring to an end the jurisdiction of the European Court of Justice in Britain"*. However, she also stated that the *"acquis"* – the body of existing EU law - would be converted into British law for the time being. This would include the judgments to date of the CJEU, including this ruling on data retention. It would only be *if* or *when* Parliament took the decision to change this aspect of EU law that the effects of this judgment on our communications data regime would cease to be felt in the UK. However, given the Secretary of State's vigorous defence of DRIPA in the judicial review proceedings, and Parliament's very recent enactment of IPA, all indicators suggest this will be a matter of "when" rather than "if".

(2) It is surprising and not wholly satisfactory that the CJEU provided no direct answer to the UK's referred questions on the correct meaning of *Digital Rights Ireland.* That case was mentioned relatively few times in the judgment, and most frequently as an aside in parentheses. At several points, after stating a proposition about the EU law of data retention which could be derived from the E-Privacy Directive, the CJEU directed the reader to "see, by analogy, with respect to Directive 2006/24 [the Data Retention Directive], the *Digital Rights* judgment". The Court did not rely on *Digital Rights Ireland* for the establishment of such general principles, instead finding itself able solely to rely on a process of reasoning from the E-Privacy Directive. Nonetheless, the judgment is at least sufficiently clear that there *are* mandatory requirements within EU law which govern domestic data retention regimes, even if it was only explained indirectly that *Digital Rights Ireland* is not the ultimate source of those requirements.

(3) The fact that the judgment has already given rise to differing interpretations suggests that it was not worded as carefully as it ought to have been. For example, Thomas Raine, writing for the UK Constitutional Law Blog (available here), understood the CJEU to be saying that only the objective of fighting serious crime was capable of justifying domestic legislation requiring the retention of communications data. Such a view would be an understandable way of resolving the ambiguity inherent in [102] of the judgment, were it not for less ambiguous statements to the contrary, for example at [90] of the judgment. The CJEU there stated that it is the objectives listed in Article 15(1) which are permissible, only one of which is fighting crime. Other acceptable options include "national security…, defence, public security … [fighting] the unauthorised use of the electronic communication system, or one of the other objectives specified in Article 13(1) of Directive 95/64". My reading, as set out above, is that the CJEU was specifying that *where fighting crime is the purpose for which domestic legislation provides for data retention*, the crime in question can only be serious crime, but this is not the only permissible purpose for which legislation can require data retention.

Given that the sole purpose of the two references seeking this preliminary ruling was to obtain clarity on the law of data retention, such ambiguity in drafting as this is particularly regrettable.

Daniel Beard QC and Gerry Facenna QC acted for the United Kingdom Government.

Azeem Suterwalla (instructed by Bhatia Best Solicitors) acted for Mr Brice and Mr Lewis.

The CJEU's judgment is available here.

The Advocate-General's Opinion is available here.

Digital Rights Ireland is available here.

The Court of Appeal's judgment is available here.

The Comment made in this case note are wholly personal and do not reflect the views of any other members of Monckton Chambers, its tenants or clients.

Monckton Chambers
1 & 2 Raymond Buildings
Gray's Inn
London, WC1R 5NR

Tel: +44 (0)20 7405 7211
Fax: +44 (0)20 7405 2084
Email: chambers@monckton.com
www.monckton.com