GlobalResearch
Center for Research on Globalization

Invalidating the Snoopers' Charter? Privacy, Surveillance and Britain's Data Retention and Investigatory Powers Act (DRIPA)

By Dr. Binoy Kampmark
Global Research, December 23, 2016

Region: Europe
Theme: Intelligence, Police State & Civil Rights

Deemed by the Home Office an exemplar of legislation balancing security and freedoms, the UK Data Retention and Investigatory Powers Act (DRIPA), otherwise known as the Snoopers' Charter, did not impress the EU Court of Justice. The case had been brought in 2014 by two MPs, David Davis and Tom Watson. Davis had since evacuated from the brief, leaving Watson to savour the proceedings.

The issue pivoted on a few crucial notions behind the requirement that communications service providers retain "traffic data" (fixed and mobile call logs) and mobile phone location data up to 12 months. These were the necessity of such an undertaking and its ultimate object. Retaining data which might become a delicious point of entry for law enforcement authorities has been a thorny subject in the context of EU laws.

Importantly, the views of governing authorities have diverged from those on the Court bench. The European Commission has been rather sympathetic to the whole idea of data retention.

In 2014, the Commission outlined its views on the subject:

> Data retention enables the construction of trails of evidence leading up to an offence. It also helps to discern or corroborate other forms of evidence on the activities of and links between suspects and victims. In the absence of forensic or eyewitness evidence, data retention is often the only way to start a criminal investigation. Generally, data retention appears to play a central role in criminal investigation even if it is not always possible to isolate and quantify the impact of a particular form of evidence in a given case.

That same year, the court struck down the European Union's own Data Retention Directive of 2006 in Digital Rights Ireland, deeming it incompatible with the fundamental rights of the European Charter.[1] Since then, an assortment of European states have tried to evade the implications of that ruling.

Keeping it a quiet domestic matter, states such as the Czech Republic, Cyprus, Estonia, Finland, France, Germany, Ireland, and Poland , all sympathetic with the British cause in this case, have deemed the Digital Rights Ireland case to be non-mandatory.[2]

The EU legislation, strictly speaking, does not prohibit such data retention regimes altogether, but it certainly takes aim at indiscriminate gathering. To accept the dragnet

concept would be to tolerate violations of privacy and the sanctity of personal information.

DRIPA had to fall within the acceptable requirements of Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council (12 July 2002), namely, the processing of personal data and the protection of privacy in the electronic communications sector.

Even more to the point, DRIPA could fall foul of various articles of the Charter of Fundamental Rights of the European Union (Art. 7, covering privacy; Art 8, dealing with the protection of personal data, and Art. 52(1), recognising that limitations to the Charter rights and freedoms must be provided for by law).

The court, to that end, found DRIPA to be unwarranted in its scope. Its machinery "exceeds the limit of what is strictly necessary and cannot be considered to be justified in a democratic society" (para. 107).

Access to such retained data must, in principle, be restricted to the purpose of preventing and detecting serious crime. This was never the exclusive purview of DRIPA, which acts as an extensive proboscis for a security establishment desperate to grabble with metadata.

Even if national legislation was provided for the purpose of fighting crime, it would be precluded if it "provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication."[3]

The court also explained that national legislation, ostensibly passed to fight crime, would also be invalid on the subject of accessing gathered traffic and location data if "access of the competent national authorities to the retained data… is not restricted solely to fighting serious crime".

That access must be subject to prior review by a court or independent administrative authority. This point is particularly important in requiring review that is not internal and sanctioned by the security fraternity.

There must also be "objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users" (para 119).

The issue of what such "objective criteria" might be furnishes agencies with a rather large bone of contention. Graham Smith, partner at law firm Bird & Bird, told The Register that, "Serious disagreements are likely over where the boundary lies between targeted and general data retention."[4] Clarity of rules, precision and effect, will be the bread and butter issues of dispute.

Other problems are also underscored. In creating a data retention regime, there are also "the appropriate technical and organisational measures" that are required "to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data" (para 122).

The Home Office claimed it was "disappointed with the judgment from the European Court of Justice and will be considering its potential implications." But the court, rather than throwing the entire surveillance project out altogether, has simply reminded the authorities

that discrimination in that field is golden.

The HO will also have another crack at matters with the English Court of Appeal. Rather than rubbishing the entire effort of the May government into legal oblivion, it has given an English court the chance to see how UK law tallies with EU requirements (para. 124).

Targeted surveillance and data retention are always more preferable to the retarding effect of a hoovering system. And it just might go some way to preserving a few fundamental human rights. Much of this will depend on what constitutes a targeted retention.

Dr. Binoy Kampmark *was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email: bkampmark@gmail.com*

Notes

[1] http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=612204
[2] https://terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/
[3] https://www.documentcloud.org/documents/3245181-C-203-15-amp-C-698-15-Arre-T-En.html
[4] http://www.theregister.co.uk/2016/12/22/did_the_eu_just_kill_the_investigatory_powers_act_heres_what_you_need_to_know/
