Blanket data retention not lawful (Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others)

09/01/2017

Corporate Crime analysis: As Tom Orpin-Massey, a barrister at QEB Hollis Whiteman Chambers, points out, given that British law enforcement and intelligence services are heavily reliant on retained archives of communications data, the ruling in Tele2 Sverige and Watson may have profound implications.

Original news

C-203/15 and C-698/15: *Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others* [2016] All ER (D) 107 (Dec)

The Court of Justice of the European Union gave a preliminary ruling, deciding, among other things, that article 15(1) of Directive 2002/58/EC, as amended by Directive 2009/136/EC, read in the light of arts 7, 8, 11 and 52(1) of the Charter of Fundamental Rights, had to be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, was not restricted solely to fighting serious crime, where access was not subject to prior review by a court or an independent administrative authority, and where there was no requirement that the data concerned should be retained within the EU.

Briefly, what is the background to this case?

The Data Retention and Investigatory Powers Act 2014 (wonderfully shortened to DRIPA 2014) made provision for the Secretary of State to require public telecommunications operators (your Vodafones, TalkTalks etc) to retain communications data for a period of 12 months. In effect, this created a regime whereby all communications data, that is the 'who', 'when', 'where' and 'how' of a communication (time date, location and type of contact)—but not the content of that communication—was routinely retained by operators and stored within a data archive.

Using their powers under the Regulation of Investigatory Powers Act 2000 (RIPA 2000), law enforcement agencies then accessed these archives for one of the purposes allowed in the Act, for example if necessary in the interests of national security or for the purpose of preventing or detecting crime.

So far so good for the government, and they were perfectly happy with that arrangement.

Step forward the 'anti-snooping' campaigners, including Labour MP Tom Watson, the Law Society, and the campaigning group Liberty. They were unhappy with this regime, arguing that it breached the privacy of ordinary folk who were having their every communications activities logged and stored away without their say so. They challenged the DRIPA 2014 provisions as being incompatible with EU law by way of a judicial review and were successful in the High Court. The government appealed to the Court of Appeal and from there the case was referred to the Court of Justice.

The Court of Justice joined the case to that of *Tele2 Sverige AB v Post-och telestyrelsen*, a similar Swedish data retention matter, and the Grand Chamber handed down its judgment on 21 December 2016.

What issues were being referred to the Court of Justice?

The question the Court of Justice had to answer was this: are national laws that impose on data providers a general obligation to retain data and then allow authorities to access that retained data for purposes not entirely restricted to the fighting of serious crime, and where access is not subject to prior review by a court or an independent administrative authority, compatible with EU law?

What did the court decide, and why?

The answer from the court was unambiguous: blanket data retention was not lawful. It held that retained data, when looked at in the round, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained. Therefore, the data attracted a fundamental right of privacy. Any interference with that right was serious. The blanket retention of the communications data of all citizens could not be lawful. Any national legislation that allowed for blanket retention therefore exceeded the limits of what is strictly necessary and could not be considered to be justified within a democratic society.

However, all was not lost for the government. The court accepted that it is necessary for Member States to retain and access communications data in certain well-established situations, the obvious examples being the protection of national security or the fight against serious crime. What it asked of the government, though, through its legislation, was to think more clearly and to be more precise as to the circumstances in which data could be retained and then accessed. Targeted rather than general data retention, for the purpose of fighting serious crime, restricted to retaining data that was strictly necessary, and accessed via appropriate safeguards, would not be unlawful.

The court was clear that such legislation must be based on objective evidence which makes it possible to identify the persons whose data is likely to reveal a link with serious criminal offences. Clearly, that is not everybody.

What are the practical implications of the decision?

Given that British law enforcement and intelligence services are heavily reliant on retained archives of communications data—indeed it is said to be used in 95% of serious and organised crime investigations and has played a significant role in every MI5 counter terrorism operation over the last decade—the ruling may have profound implications.

What the Grand Chamber in *Watson and others* appears to be asking for is more focus, more specificity, and better procedural safeguards as to accessing communications data than was evidenced in DRIPA 2014 (and now in the Investigatory Powers Act 2016 (IPA 2016)). The government is casting its net too wide, and with too little caution, encroaching on the rights of privacy of ordinary people.

What is likely to happen next? Nothing until the Court of Appeal returns to session and considers the judgment, and then decides how to apply it to the judicial review matter before it. Brexit poses another question. Will the government consider itself to be bound by such determinations when drafting future powers? It seems likely, however, in the short term at least, that the government will work on emergency legislation, possibly by way of amendment to IPA 2016, to ensure that the police and security services have continued recourse to data retention, albeit perhaps now in a far more limited way.

How does the decision sit with the new data retention provisions of IPA 2016?

IPA 2016 has incorporated the data retention powers of DRIPA 2014 at IPA 2016, Pt IV. Indeed, IPA 2016 significantly expands the data retention regime by also expressly including internet connection records at IPA 2016, s 87(11), an allowance that had not been spelled out in DRIPA 2014. This is a significant expansion of the definition of communications data and led in large part to IPA 2016 being labelled the ‘snoopers charter’ by privacy campaigners.

Should the Court of Appeal determine that these retention provisions are not compatible with EU law, the government would seem to need to amend IPA 2016 significantly to make it compliant. This will require the drafting of further clauses to qualify the circumstances in which data retention will be lawful.

Any other points of interest?

The Court of Justice reminded us in their judgment that it wasn’t just the fight against crime that could justify data retention, it was the fight against serious crime. What is serious crime? IPA 2016 defines it as an offence which could attract a custodial sentence of three years or longer. This significantly narrows the purpose for which data can be retained and accessed, and the bodies that might request access to such data. Gone may be the days when a wide range of public authorities could access retained data with relative ease.

Tom Orpin-Massey accepts instructions in all areas of chambers’ work, as an advocate or in an advisory capacity—notably in general crime, business crime, regulatory and legal professional privilege.

Interviewed by Kate Beaumont.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor

CLICK HERE FOR A FREE TRIAL OF LEXIS®PSL

About LexisNexis | Terms & Conditions | Privacy & Cookies Policy
Copyright © 2015 LexisNexis. All rights reserved.