# Data retention: Greater focus, specificity, and more safeguards

The European court's snooping judgment was not a total victory for the privacy lobby, explains **Tom Orpin-Massey**

Tom Orpin-Massey is a barrister at QEB Hollis Whiteman
@QEBHW
www.qebholliswhiteman.co.uk

**Privacy campaigners received an early Christmas present on 21 December 2016 when the Grand Chamber of the Court of Justice of the European Union (CJEU) ruled that the blanket retention of communications data at the behest of the state was unlawful.**

Labour MP Tom Watson, the Law Society, and other privacy groups had keenly awaited the court's decision in the joined cases of *Sverige AB v Post-och telestyrelsen*, a Swedish matter, and *Secretary of State for the Home Department v Tom Watson and Others*, a British judicial review.

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 per cent 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. Is this the end of mass data retention?

A bit of background first. The Data Retention and Investigatory Powers Act 2014 (DRIPA) made provision for the secretary of state to require public telecommunications operators to retain communications data for a period of 12 months. In effect, this created a regime whereby all communications data – the who, when, where, and how, but not the content of, a communication – was routinely retained by operators and stored within a data archive.

Using their powers under the Regulation of Investigatory Powers Act 2000 (RIPA), law enforcement agencies could then access this archive for one of the purposes allowed in the Act, for example in the interests of national security or for the purpose of preventing or detecting crime. So far so good for the government, and it was perfectly happy with that arrangement.

Step forward the 'anti-snooping' campaigners. Unhappy with the regime, and arguing it to be a breach of the privacy of ordinary folk who were having their every phone or computer activity logged and stored away without their say so, they challenged DRIPA by way of a judicial review. The matter progressed to the Court of Appeal and subsequently to the CJEU for a determination on compatibility with EU law.

The question the CJEU 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?

The answer from the court was unambiguous: no. 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. A total victory for the privacy lobby? Not quite.

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 was to think more clearly and to be more precise as to the circumstances in which data could be retained and 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 the court appears to be asking for is more focus, more specificity, and better procedural safeguards to accessing communications data than is presently evidenced in DRIPA. 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 consider and then decides how to apply the CJEU's judgment, if at all, to the judicial review still before it.

Brexit poses another question. Will the government consider itself bound by such determinations when drafting future powers? It seems likely, in the short term at least, that the government will work on emergency legislation, possibly by way of amendment to the Investigatory Powers Act 2016, to ensure the police and security services have continued recourse to data retention, albeit perhaps now in a far more limited way. **SJ**