Back to the drawing board thanks to the CJEU's judgment in Watson & Ors

Michael Drury and **Julian Hayes** explain why already repealed data retention legislation is still causing the UK Government a headache.

On 21 December 2016, the European Court of Justice (CJEU) handed down its long awaited decision in a high-profile privacy challenge brought by MP Tom Watson and others. The judgment took the shine off the Government's newly enacted Investigatory Powers Act (IPA).

The challenge had been brought against the Data Retention Investigatory Powers Act 2014 (DRIPA) which empowered the Secretary of State to require telecoms operators to retain relevant telecommunications data (for example, data necessary to identify the source, destination, time, date, duration and type of a communication) for reasons such as national security, the prevention or detection of crime and the prevention of disorder.

Given that DRIPA contained a "sunset clause" causing it to expire on 31 December 2016 anyway, the proximity of the CJEU judgment to the Act's expiry might have consigned *Watson & Ors* to relative legal obscurity, had not DRIPA's provisions been substantially incorporated into the IPA, the data retention sections of which were brought into force on 30 December 2016. As a result, the judgment has become highly significant to the Government, to law enforcement capability (and by extension the general public) and to telecoms operators receiving IPA retention notices in future.

The CJEU Judgment

In giving judgment, the CJEU explained the significance of the data concerned. It allowed very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained – their everyday habits, places of residence, daily movements, activities and social relationships. Taken as a whole, the DRIPA retention requirements represented a particularly serious and far-reaching interference with the EU Charter rights to respect for private and family life and for the protection of personal data.

Interference with such fundamental rights must be clear and precise in scope and application and must be strictly necessary and proportionate to the end sought, be that safeguarding national security, defence and public security or the prevention, detection and prosecution of crime. Where the aim is the fight against crime, only serious crime justifies the interference with EU Charter rights. Most significantly, the fight against serious crime, in particular organised crime and terrorism, could not alone justify national legislation providing for *"the general and indiscriminate retention of all traffic and locations data"*.

Whilst the general retention of data infringes EU Charter rights, national laws could permit the *targeted* retention of data if, based on objective evidence, it were first possible to identify a section of the public whose data is likely to reveal at least an indirect link with serious criminal offences or prevent a serious risk to public security.

Targeted retention might be justifiable where there is a high risk that individuals in a particular geographical area might be involved in preparing to commit a serious crime. The Court did not give guidance on the potential size of such geographical areas, nor did it expressly exclude the possibility that other limits besides geography

might be applied if objective data justifies it. This unhelpfully opens up the damaging possibility that a member state could seek in future to retain data on the basis of ethnicity or religion, causing potential friction with equalities legislation, although doubtless the CJEU will require something more precise to justify selection on objective evidence.

Where targeted data is retained, access to it must correspond to the criterion for its retention – where crime fighting is concerned, *"only the objective of fighting serious crime is capable of justifying such access to the retained data".* Generally, access can only be granted to the data of individuals suspected of either planning to commit, having committed, or being implicated in connection with a serious crime. However, in an ambiguous passage highlighting the tension which many people feel between the competing priorities of privacy and combating crime (particularly after recent violent atrocities in Europe), the CJEU stated that access to the data of individuals who are not suspects might also be granted where it could be shown that it would make an "effective contribution" in combating specific terrorist threats to vital national security, defence or public security interests.

Perhaps the clearest and most crucial element of the judgment is that access to retained data must be proportionate and must normally be authorised by a Court or independent administrative body. Data subjects must be notified if their data has been accessed once doing so would no longer jeopardise an ongoing investigation. Finally, in a move with potential practical implications for telecoms operators served with retention notices, national legislation must make provision for retained data to be held within the EU. This latter point is a new and potentially significant development.

Impact on the IPA

Watson & Ors places the CJEU on an immediate collision course with the IPA. At present, Part 4 of the IPA permits the retention of data for a whole raft of reasons besides national security and crime fighting, including the protection of public health, assisting in investigations of miscarriages of justice, assisting in identification of someone who has died or who is too ill to identify themselves, for the regulation of financial markets and for the collection of taxes.

As a result of the CJEU decision, none of these reasons will legally justify data retention even though many people may regard them as justifiable.

Similarly, retention notices requiring the retention of "all data or any description of data" may now be too broad without qualification by reference to a geographical limit based on a particular threat. However, as the UK's Independent Reviewer of Terrorist Legislation has indicated, because suspects are often not known in advance, the more limited data retention now permitted may well miss the perpetrators of offences who had not previously come to the attention of the authorities and who could not, therefore, be targeted in advance. In other words, non-universal data retention will inevitably be less effective as a crime fighting measure (or as a means of preventing atrocities that are in themselves seen as crimes as well as threats to national security). It is a matter of ongoing moral debate whether the collateral intrusion on the data of innocent people inherent in the generalised data retention, as advocated by the UK Government, is a price worth paying in the fight against crime.

When Part 3 of the IPA comes into force, a designated senior officer from one of 48 public authorities will have the power to grant access to retained data for the purpose of a specific investigation or operation for a number of statutory reasons. Such powers are likely to be challenged by privacy campaigners at an early

opportunity. Real questions arise about the compatibility of the IPA and the existing RIPA requests that still remain in force.

Finally, the requirement to notify data subjects that their personal data has been accessed once an operation is over risks placing a costly administrative burden on the authorities responsible, potentially undermines the effectiveness of future security operations and may overwhelm and alarm those receiving such notification.

Outlook

The matter now returns to the UK's Court of Appeal for a decision on the operation of DRIPA (and by implication the IPA's data retention provisions). In due course, it is likely that the Government will have to amend the IPA. In the meantime, those tempted to look to Brexit as a solution to the legislative dilemma may be disappointed; if Britain wishes to maintain the free flow of data with member states after its eventual departure from the EU, it will be obliged to provide "essentially equivalent" data protection to that provided within the EU; a refusal to amend the IPA in conformity with this and future CJEU judgments may well curtail such data flows with significant consequences for the UK's economy.

Michael Drury & Julian Hayes

BCL