Privacy v security

Nicholas Griffin QC

considers the CJEU *Watson* decision on UK surveillance law

© Istockphoto/pixinoo

IN BRIEF

- A recent CJEU decision addresses an important aspect of UK surveillance law and finds it wanting.
- It raises questions about the current UK regime governing the retention of and access to data about our communications.
- The government says its approach is a necessary part of the fight against crime and terrorism. However, the view of privacy campaigners—that the law goes too far—found support at the CJEU.

The Court of Justice of the EU (CJEU) delivered a judgment just before Christmas that is full of significance for the government's approach to surveillance and the fight against crime and terrorism. It did so in the *Watson* case (in fact joined cases *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and others*, C203/15 and C698/1 of 21 December 2016). The decision is a major victory for privacy campaigners such as MPs Tom Watson and David Davis, who were behind the case from its inception. It has serious implications for government policy requiring the blanket retention of information about our communications by service providers. This provides a pool of data into which law enforcement agencies can dip when necessary.

The judgment goes to the heart of the sensitive and difficult balancing exercise the government must undertake between ensuring the privacy of its citizens on the one hand and their safety and security on the other. The government must strike this balance at a time of heightened concern post-Snowden of significant privacy breaches—but also at a time of heightened concern about terrorism, as underlined by the killing of 12 people in a Berlin Christmas market just two days before the judgment came out.

The decision has additional resonance in Brexit Britain as it entails European judges reaching binding conclusions in relation to Westminster law. And, while the central reasoning of the CJEU is clear, the finer details of the judgment may add to the controversy by advocating an approach that is itself open to criticism.

Communications data

The CJEU was considering the Data Retention and Investigatory Powers Act 2014 (DRIPA 2014), s 1 of which creates powers regarding the retention of "communications data", which is helpfully described in DRIPA 2014's explanatory notes as: "The context not the content of a communication. It can be used to demonstrate who was communicating; when; from where; and with whom. It can include the time and duration of a communication, the number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. It does not include the content of any communication: for example the text of an email or a conversation on a telephone."

It is generally agreed that access to this data forms a significant weapon in the armoury of the law enforcement organisations and intelligence agencies and has led to convictions in criminal cases on countless occasions.

As we increasingly lead our lives online and communicate electronically, we leave an ever-greater digital trail. It is now possible to learn a great deal about who we are by accessing our communications data. As the CJEU observed in the *Watson* case: "That data…is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them…In particular, that data provides the means…of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."

EU Charter & data protection

Central to the *Watson* case was the CJEU's consideration of the fundamental privacy rights contained within Arts 7 and 8 of the Charter of Fundamental Rights of the European Union. Article 7 guarantees the respect for private and family life, home and communications in very similar terms to Art 8(1) of the European Convention on Human Rights. The Charter, which is prized by the European Commission as a modern codification, also includes "third generation" rights including data protection. The right to protection of personal data is recognised by Art 8, which specifies that such data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law".

Article 52(1) sets the boundaries for permissible derogation from such fundamental rights. Any limitation must be provided for by law and respect the essence of those rights; "limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others", subject to the principle of proportionality.

The Data Protection Directive (95/46/EC) had also mapped out the requirements of member states to protect their citizens' right to privacy with respect to the processing of personal data.

The e-Privacy Directive (2002/58/EC) applies its principles to the processing of personal data specifically in the electronic communication sector. Article 5(1) requires member states to prohibit the surveillance of communications and related traffic data without the user's consent.

Both directives make provision for derogation for the prevention, investigation, detection and prosecution of criminal offences and in other specified circumstances, such as safeguarding national security. Article 15(1) of the e-Privacy Directive specifies that restrictions must be necessary, appropriate and proportionate in a democratic society.

The Data Retention Directive & Digital Rights Ireland

A number of EU countries had indeed acted to restrict the full application of the data protection provisions. They brought in legislation requiring the retention of data by service providers on the basis that this was necessary for the prevention etc. of criminal offences. The Data Retention Directive (2006/24/EC) aimed to harmonise the different national approaches. It did so by *requiring* member states to adopt measures to ensure that communications data was retained by communications service providers for at least six months and up to two years (Arts 1-6).

Many felt the Data Retention Directive was out of kilter with the balanced approach of the Charter and above directives. And in 2014 the CJEU invalidated it in the *Digital Rights Ireland* case [2015] QB 127, [2014] 2 All ER (Comm) 1, holding that the Directive entailed a wide ranging and particularly serious interference with privacy rights and the protection of personal data, which was not limited to what was strictly necessary. The court held that the Directive failed to provide sufficient safeguards to ensure effective protection of the data and did not ensure the irreversible destruction of the data at the end of the data retention period.

DRIPA 2014

The UK coalition government decided to legislate to replace the powers contained in the domestic regulations implementing the invalidated Data Retention Directive. The resulting DRIPA 2014 replicated the requirement for the mandatory retention of communications data by public telecommunications operators, for up to a year (s 1), but supposedly with new and sufficient safeguards. The retention requirement was triggered by a notice issued by the home secretary, where necessary and proportionate for the purposes set out in s 22(2) of the Regulation of Investigatory Powers Act 2000. These include the prevention or detection of crime and other purposes such as national security.

DRIPA 2014 was fast-tracked through Parliament with Labour support but, others argued, minimal scrutiny. David Davis MP complained that the government was "treating the entire nation as suspects" with this legislation. He and Tom Watson MP teamed up and brought successful judicial review proceedings challenging s 1 of DRIPA 2014 in EU law, in reliance on *Digital Rights Ireland* and the rights under Arts 7 and 8 of the Charter (*R (Davis) v Secretary of State for the Home Department* [2015] EWHC 2092 (Admin), [2015] All ER (D) 180 (Jul)).

The government appealed. The Court of Appeal was more sympathetic to their case and particularly their argument that *Digital Rights Ireland* did not impose mandatory requirements which must be applied to national legislation. However, it decided to refer this question to the CJEU for a preliminary ruling (*Secretary of State for the Home Department v R (Davis)* [2015] EWCA Civ 1185, [2015] All ER (D) 196 (Nov)).

CJEU

All of which brings us to the *Watson* decision. The CJEU held that the EU Charter and Directives preclude national legislation which provides for: (a) general and indiscriminate retention of communications data of for the purpose of fighting crime; and (b) access to the retained data by national authorities where that access was not restricted to the purpose of fighting *serious* crime, was not subject to prior review by a court or independent authority (save in cases of urgency) and where there was no requirement to retain the data in the EU.

The CJEU said that national legislation must "indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary". Further, the retention of data "must…meet objective criteria, that establish a connection between the data to be retained and the objective pursued".

The court accordingly set out a list of the requirements under EU law for the permissible retention of and access to communications data in the context of fighting crime, in comparison to which DRIPA 2014 would be found wanting.

The Home Office is "disappointed" with the ruling but privacy campaigners have understandably met the decision with joy. Tom Watson said that the ruling "shows it's counter-productive to rush new laws through Parliament without a proper scrutiny".

Controversy

The decision is controversial in a number of respects:

- The CJEU recognises in its decision the general interest in using modern investigative techniques in the fight against organised crime and terrorism—but concludes that such an objective cannot of itself be sufficient to justify the blanket approach of legislation such as DRIPA 2014. Others would not agree.
- The court requires a more targeted law based on objective evidence making it possible to identify those whose data is likely to reveal a link with serious crime. But how might this be achieved? The Court says that limits may be set "by using a geographical criterion where the competent national authorities consider … that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences". It is not entirely clear what this means. David Anderson QC, the Independent Reviewer of Terrorism Legislation, has pointed out that the general retention of data generated by people in a particular location, such as a housing estate, could be seen as geographical profiling, which would raise its own "extremely sensitive legal and ethical issues".

- Arch-Brexiteer David Davis MP was one of those behind the DRIPA 2014 challenge which propelled the case to Luxembourg (although he dropped out on being appointed to the Cabinet). The CJEU decision constitutes the binding conclusions of European judges in respect of the validity of Westminster legislation. This would therefore presumably amount to just the type of "outside interference" that many Brexit supporters have complained about.
- Why was the CJEU considering domestic provisions aimed at fighting crime, terrorism and the like at all? Surely, these are security matters, which should be within the province and responsibility of national governments. The CJEU is, or should be, concerned with the processing of personal data in the course of activity falling within EU law. The English Court of Appeal had considered a similar question before referring the case to the CJEU, concluding that provisions in relation to access fell within the scope of EU law and had to be evaluated by reference to the Charter and other general EU law principles.

This also gives rise to the question whether we will actually be able to ignore important CJEU decisions concerning data protection post-Brexit. Perhaps not. It is being suggested by the Information Commissioner and others that we should assume that the EU will continue to require minimum standards with regard to data protection from the UK in exchange for a meaningful relationship with Europe.

Court of Appeal

The formal process is now for the case to go back to the Court of Appeal, which will apply the CJEU decision in its consideration of the validity of DRIPA 2014. The Home Office will apparently continue to contest the case on the basis that the communications data regime is sufficiently robust and compliant.

A twist in this case is that DRIPA 2014 contains a sunset clause by which its data retention provisions expired at the end of 2016. The English litigation and the CJEU decision were therefore all in relation to law that is no longer in force.

Much of the CJEU decision's significance in fact derives from its potential effect not on DRIPA 2014 but on the legislation that replaced DRIPA 2014: the Investigatory Powers Act 2016. Its data retention provisions are now partially in force and repeat important aspects of the approach in DRIPA 2014, albeit subject to an amended oversight framework. The real headache for the government therefore comes with the suggestion that the new legislation does not comply with EU Charter and law requirements. **NLJ**

Nicholas Griffin QC practises from QEB Hollis Whiteman. He is former chair of the Bar Council Surveillance and Privacy Working Group (*www.qebholliswhiteman.co.uk*)