RETENTION OF COMMUNICATIONS DATA: ARE WE THERE YET?

With the underlying EU Data Retention Directive ruled invalid, new UK legislation rushed onto the statute books to replace it, and further changes being recently introduced, is the upheaval yet over for retention of communications data laws?

THE RECENT INTRODUCTION OF NEW DATA RETENTION powers in the Counter-Terrorism and Security Act 2015 is the latest development in a period of unprecedented upheaval for data retention legislation. This article takes stock of the changes to date and considers the future direction of travel of this topical area of law in the current post-Snowden political climate.

The principle of data retention legislation is to oblige companies providing communications networks or services to the public to retain the "metadata" relating to their customers' communications for a period of time so that it can be made available to intelligence services and law enforcement agencies in the course of a criminal investigation or a secret intelligence operation. Metadata is typically described as the 'who, where, when and how' of a communication, but not its content. The term is broad, for example often encompassing geo-location data relating to mobile phones, and IP addresses assigned to devices accessing the internet.

> The current legislative framework governing the intrusive capabilities of the UK's intelligence services needs a complete overhaul

Until April 2014, data retention in the EU was underpinned by a legal framework established by the Data Retention Directive (2006/24/EC). The Directive was introduced in the midst of heightened national security concerns about the threat of international terrorism in the first part of the last decade. It was transposed into law in the UK by the Data Retention (EC Directive) Regulations 2009 (the 2009 Regulations).

The Directive required providers of publicly available electronic communications services or public communications networks to retain certain types of metadata relating to their customers for a period of time of between six months and two years. This obligation was carved out of the existing overarching rule that customer metadata could be retained only for the time necessary to enable a communication to take place or for invoicing-related purposes.

On 8 April 2014, the Court of Justice of the European Union (CJEU) ruled that the Directive was invalid. Following a few months of uncertainty in the UK about the legal status of the 2009 Regulations, on 10 July 2014, prime minister David Cameron announced emergency new primary legislation to replace them.

The Data Retention and Investigatory Powers Act 2014 (DRIPA) passed into law just seven days later under the emergency fast-track legislative process. The accompanying Data Retention Regulations 2014 (the 2014 Regulations) came into force on 31 July 2014. DRIPA's data retention provisions were then extended by the Counter-Terrorism and Security Act 2015, which received Royal Assent on 12 February 2015. By any yardstick, the pace of legislative change in the UK has been rapid.

An invalid Directive

The CJEU's declaration of invalidity was the conclusion of its judgment in the case of *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* C-293/12 joined with *Karnter Landesregierung* C-594/12. The two joined cases were preliminary references from the Irish and Austrian courts. Each court asked the CJEU to clarify, among other things, whether the Directive was compatible with two fundamental rights enshrined in the EU Charter of Fundamental Rights (the Charter):

- Article 7 (the right to respect for a person's private and family life, home and communication); and
- Article 8 (the right to the protection and fair processing of a person's personal data).

The CJEU found that the obligation imposed by the Directive to retain customer metadata was itself an interference with the privacy rights guaranteed by Article 7 of the Charter. The provision of access to this data to intelligence and law enforcement agencies was a further interference with Article 7 rights. In providing for the processing of personal data, the Directive also interfered with the fundamental rights granted under Article 8.

The CJEU's description of the Directive was startlingly unequivocal: its interference with Articles 7 and 8 was "wide ranging, and... particularly serious" and "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance". In short, the Directive constituted "an interference with the fundamental rights of practically the entire European population".

Nonetheless, the CJEU did make it clear that meeting the objectives of the Directive could in theory be a ground for a justifiable limitation of Charter rights. It found that because the Directive did not allow access to the content of communications, it did not adversely affect the essence of the Article 7 and Article 8 rights. It also recognised that fighting international terrorism and serious crime are objectives of general interest that might justify limiting such rights.

Instead, the focus of the CJEU's criticisms was on the Directive's lack of proportionality, particularly its imprecise scope and its failure to limit its own interference in the Charter rights. The judgment contained a long list of deficiencies, with some key themes being that the Directive:

- was too generalised and overly broad in scope, without any level of differentiation, limitation or exception;
- set no limits or conditions to the access granted to competent national authorities to the relevant data, or their subsequent use of it; and
- did not contain any rules relating to security, protection or destruction of data in light of the vast volumes of data (much of it sensitive) retained.

Uncertainty ensues

As might be expected, the judgment created considerable uncertainty. Although EU data protection regulators and privacy advocates welcomed the decision, from the UK government's point of view, the prospect loomed of telecommunications service providers unilaterally deciding to stop retaining metadata, and then deleting what they had retained in order to comply with data protection laws.

The UK unveils DRIPA

Even so, when the UK government announced DRIPA, to some surprise, it stated that DRIPA was not only necessary in order to plug the legislative hole created by the Directive's invalidity, but also to address another issue that threatened to undermine the legal basis of the government's investigatory powers: the scope of the Regulation of Investigatory Powers Act 2000 (RIPA) was being challenged by various (unnamed) telecommunication service providers based outside the UK.

RIPA is the UK legislation under which the intelligence services, law enforcement agencies and to a limited extent other government bodies can be granted powers to secretly monitor individuals, including to intercept communications, acquire metadata of communications (now retained under DRIPA) and undertake covert surveillance.

The UK government did not provide much detail about the nature of the challenges to RIPA. Nevertheless, DRIPA's amendments (described as 'clarifications' by the government) gives RIPA (among other things) an explicitly extra-territorial reach. It ensures that any communications service provider anywhere in the world that offers communication services to customers in the UK can be served with an interception warrant under RIPA, which may include the requirement that action to implement the warrant be taken outside the UK.

Other amendments related to RIPA's defined terms. RIPA has always used a different set of definitions to describe the components of a communications network or service than those introduced in the EU Framework Directive (2002/21/EC) and then used in subsequent EU legislation relating to the telecommunications sector, including in the 2009 Regulations.

DRIPA not only uses RIPA's definitions rather than those from the 2009 Regulations, it also amends one of the most important ones within RIPA: that of 'telecommunication service', by supplementing the existing definition of "any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system" so that this includes a service that "consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted by means of a such a system".

It is hard to avoid the conclusion that this small change may have far-reaching effects in practice. The amendment appears to bring the IT infrastructure underpinning internet communications platforms and services anywhere in the world under the potential scope of RIPA. Such infrastructure may include, for example, data centres in the US supporting popular email, video calling and social media software applications.

Thus, from the UK government's point of view, DRIPA killed two birds with one stone by implementing a single legislative solution to two potentially serious legal difficulties. From the point of view of DRIPA's critics, the fact it was ushered through the legislative process so quickly, while going beyond replacing the 2009 Regulations to make far-reaching amendments to RIPA, only intensified the suspicion that a significant expansion of the government's investigatory powers has been smuggled onto the statute books without the opportunity for proper public debate or parliamentary scrutiny.

DRIPA's powers extended

The Counter Terrorism and Security Act amends DRIPA by adding a new category of metadata to it: relevant internet data. This is defined to mean data that may be used to identify, or assists in identifying, an IP address used to access the internet, or other "identifier". The drafting of the Act is not always easy to follow, but it seems that this is intended to include port numbers or MAC addresses of devices.

The amendments are cast as an attempt to solve the investigatory hurdle posed by the sharing of IP addresses, whereby a temporary IP address is automatically allocated to many customers simultaneously, making it impossible to definitively link a subscriber's device to the IP address at any point in time. The identity of websites visited, or of individual browsing histories, has been explicitly excluded.

More laws to come?

To its critics, DRIPA, the 2014 Regulations and the Counter-Terrorism and Security Act fail to replace the 2009 Regulations with a mandatory data retention regime that adequately accommodates the criticisms of the Directive made by the CJEU.

Although some safeguards have been introduced in DRIPA, notably in relation to data security measures, the detail of the obligations to be imposed is left to the discretion of the Secretary of State on a case-by-case basis. This leaves DRIPA vulnerable to judicial review on the basis of incompatibility with the Charter. Indeed, the human rights organisation Liberty has been granted permission to launch such a judicial review of DRIPA.

The UK government's position is that DRIPA is a temporary stop-gap measure. It contains a sunset clause that means the Act is automatically repealed on 31 December 2016. On 12 March 2015, the first official indication was made of what might replace DRIPA, when the Intelligence and Security Committee (ISC), which has statutory oversight of the UK's secret intelligence services, published its much anticipated *Privacy and Security Report*.

The ISC's report had little to say on the question of DRIPA's compatibility with the Charter. However, it concluded that the current legislative framework governing the intrusive capabilities of the UK's intelligence services needs a complete overhaul. It recommended that the relevant laws (including DRIPA and RIPA) be replaced by a new, transparent, legal framework under a single Act of Parliament, and that this process should start early in the next parliament.

Assuming that the government follows this recommendation, it is to be hoped that the passage of the new draft Bill envisaged by the ISC follows a more consensual and transparent process than was the case with the current data retention regime.

Charlie Hawes *is an associate and* ***Mark Taylor*** *is a partner at Hogan Lovells International LLP*