WILLIAM FRY

// TECHNOLOGY

A UK Adequacy Decision is (even) More Uncertain due to Recent CJEU Rulings on EU Privacy Law

November 2020

Mass surveillance conducted by European Union (EU) Member State national security services should operate within the bounds of the EU's privacy laws. The Court of Justice of the European Union (CJEU) recently delivered two landmark decisions involving the UK, France and Belgium where national governments have access to individuals' data in circumstances where national security is at risk. This may have significant impact on the European Commission's adequacy determination for the UK after they leave the EU in January 2021. In this briefing we explore the judgments of the CJEU and their effects on Privacy law and on the UK.

Until recently, EU Member State's national surveillance programs were considered outside the scope of EU privacy laws such as Directive 2002/58/EC on privacy and electronic communications (**ePrivacy Directive**). Article 4(2) of the EU's founding Treaty (**TEU**) states that "national security remains the sole responsibility of each Member State." However, in recent years, the CJEU has expanded the scope of individual privacy protections contained in the Charter of Fundamental Rights of the European Union (**EU Charter**) as well as EU legislation.

In 2017, the CJEU extended the reach of EU privacy protections to national legislation that enables mass surveillance for law enforcement purposes. In the decision of ***Tele2Sverige and Watson*** which followed on from the ***Digital Rights Ireland*** case, the CJEU held that Member States could not engage in "general and indiscriminate retention of metadata" for lengthy periods of time. This showed the CJEU's willingness to set limits on member state's policing activities which historically were reserved for the member state legislature.

On 6 October 2020, the CJEU delivered judgment in two landmark decisions *(case C-623/17, Privacy International, and joined cases C-511/18, La Quadrature du Net and others, C-512/18, French Data Network and others, and C-520/18, Ordre des barreaux francophones et germanophone and others)* (**Judgments**) concerning the lawfulness of legislation in certain member states which required providers of electronic communications services to forward users' traffic data and location data to a public authority, or to retain such data.

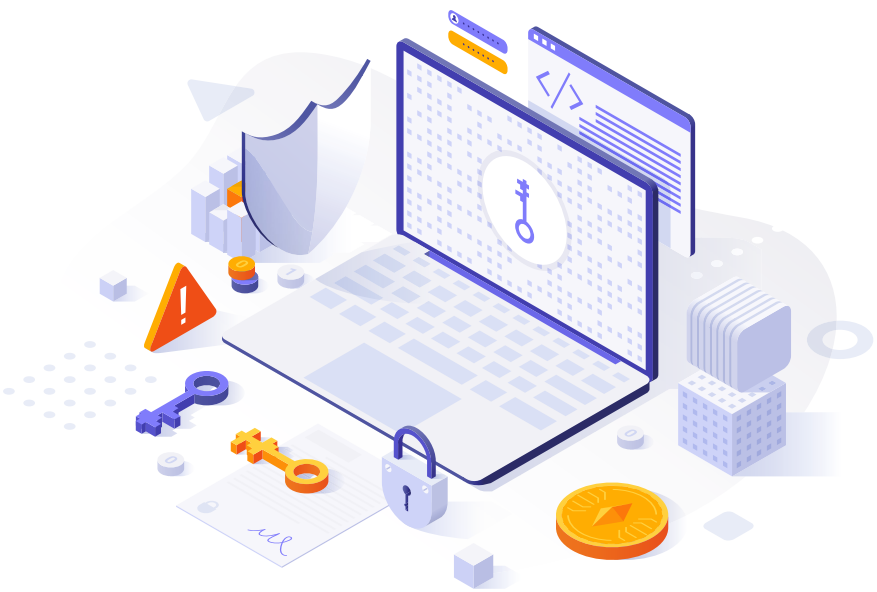
The Judgments come at a tumultuous time for the UK as it awaits an adequacy decision from the European Commission on the transfer of data between the EU and the UK, following the end of the Brexit transition period.

ENCRYPTION – WHO HOLDS THE KEY?

The Judgments may affect the cases arising out of the EncroChat 'hack' earlier this year. It may also affect the tech industry companies that use end-to-end encryption for their platforms (such as WhatsApp and Facebook) to protect their customers privacy rights. Such companies must balance privacy rights against governments' requests for data on national security grounds provided for under national legislation, such as the UK's Investigatory Powers Act 2016 (**2106 Act**).

Encryption has created difficulties for law enforcement agencies in a number of jurisdictions, including the US and UK, in terms of accessing information on phones or computers to progress a criminal investigation. Governments, in the interest of national security have previously sought the creation of "backdoors" in encryption algorithms to enable access to protected information. Tech companies however have resisted these requests, arguing that formal backdoors could undermine consumers privacy rights.

Encryption is also used by criminals to communicate and run their operations. EncroChat, an encrypted network of WIFI enabled mobile devices was hacked this summer through a collaborative effort by UK and French national authorities. The UK's National Crime Agency (**NCA**) stated that the EncroChat network had been breached in April of this year. The encrypted phones were largely used by criminals. Through this breach, the authorities were able to monitor criminal activity and make necessary arrests throughout the UK and EU. Interestingly, the data was 'intercepted' as defined under the 2016 Act, yet intercepted evidence cannot be relied on in criminal cases in the UK by virtue of section 56(1) of the 2016 Act.



THE CJEU'S LANDMARK DECISIONS

The CJEU confirmed in its Judgments that the ePrivacy Directive applies to national legislation which requires providers of electronic communications services (e.g. telecommunications companies and internet service providers, (**Providers**)) to retain or transmit personal data to intelligence authorities. The CJEU also held that member states cannot restrict the scope of the ePrivacy Directive unless such restrictions comply with the general principles of EU law, are proportionate, and preserve the fundamental rights guaranteed under the EU Charter.

The Judgments are important because they confirm that EU law applies to mass surveillance in the UK and other member states with similar domestic legislation. It applies when the member state's government compels providers of electronic communications services to process data (forwarding traffic and location data), even when processed for the purposes of national security.

C-623/17 - PRIVACY INTERNATIONAL
(PRIVACY INTERNATIONAL JUDGMENT)

Privacy International argued that having regard to the guidance derived from the case-law, both the acquisition of data by the security and intelligence agencies from those Providers and the use of that data by those agencies, falls within the scope of the ePrivacy Directive, whether that data is acquired by means of a transmission carried out in real-time or subsequently. It also argued that the fact that the objective of protecting national security is explicitly listed in Article 15(1) of the ePrivacy Directive does not mean that the directive does not apply to such situations and that assessment is not affected by Article 4(2) TEU.

In response, the United Kingdom, Czech and Estonian Governments, Ireland, and the French, Cypriot, Hungarian, Polish and Swedish Governments argued that the ePrivacy Directive does not apply to the national legislation at issue in the main proceedings, as the purpose of that legislation is to safeguard national security, which is outside the scope of the ePrivacy Directive. They further argued that those provisions are reflective of Article 4(2) TEU.

The CJEU held that Article 1(3), Article 3 and Article 15(1) of the ePrivacy Directive, read in the light of Article 4(2) TEU, must be interpreted as meaning that national legislation enabling a State authority to require Providers to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security, falls within the scope of that directive.

The CJEU further held that the ePrivacy Directive must be interpreted as precluding national legislation enabling a State authority to require Providers to carry out the "general and indiscriminate" transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.

JOINED CASES: C-511/18, LA QUADRATURE DU NET AND OTHERS, C-512/18, FRENCH DATA NETWORK AND OTHERS, AND C-520/18, ORDRE DES BARREAUX FRANCOPHONES ET GERMANOPHONE AND OTHERS (**FRENCH DATA NETWORKS JUDGMENT**)

In the joined cases involving France and Belgium, the CJEU decided that EU law precludes national legislation requiring Providers to carry out the "general and indiscriminate retention of traffic data and location data as a preventative measure". These transmission and retention activities were held by the CJEU to be "particularly serious interferences with the fundamental rights guaranteed by the Charter" in circumstances where there is no link between the individuals whose data is affected, and the objective pursued by the national legislation in question.

Notwithstanding, the CJEU clarified a number of points on scope of the ePrivacy Directive. It held that the ePrivacy Directive does not prevent:

1. an order requiring Providers to retain, generally and indiscriminately, traffic and location data in circumstances where the member state is facing "a serious threat to national security that proves to be genuine and present or foreseeable", providing that the order in question is limited to what is "strictly necessary" and must be subject to "effective review" by a court or independent body
2. legislative measures allowing the targeted retention of traffic and location data which is limited both
    a. "on the basis of objective and non-discriminatory factors according to the categories of persons concerned or using a geographical criterion", and
    b. to what is "strictly necessary"
3. legislative measures allowing the expedited retention of data where it is necessary to retain such data to shed light on established or reasonably suspected "serious criminal offences or attacks on national security";
4. legislative measures which require real-time collection of traffic and location data which is limited to persons against whom there is, following a review having been carried out by a court or independent body, a "valid reason to suspect" they are involved in terrorist activities, and
5. as to national law that is incompatible with EU law, national courts may not rely on such national legislation to "limit the temporal effects of a declaration of illegality which [they are] bound to make" in respect of national legislation requiring Providers to generally and indiscriminately retain traffic and location data.

The CJEU concluded by clarifying that, in the context of criminal law proceedings, it is for national courts to assess and determine the admissibility of evidential data against suspects, which was obtained by way of a retention of such data contrary to EU law. The same however cannot be said for evidential data which is obtained by means of a "general and indiscriminate retention of traffic and location data in breach of EU law".

BREXIT & THE EU: ADEQUACY NOW HANGING IN THE BALANCE

The making of an adequacy decision by the Commission in respect of the UK is the preferred outcome. However, it appears that an adequacy decision will be a longer process than the Brexit negotiations themselves and the 'transition period' may be extended further regarding data transfers only until a decision is made by the Commission.

According to the UK government, on exit the UK's data protection laws and frameworks will be aligned with GDPR. However, the following challenges remain:

- The 2016 Act allows for broad interception, interference and communications acquisition powers so as to limit the rights of individuals. The 2016 Act may contravene the underlying human rights principles of the GDPR. The Judgments suggest that this issue will be a continuing one for the UK. The French Data Networks judgment clarifies the scope of the ePrivacy directive, which may bring the 2016 Act outside the scope of the ePrivacy Directive in some circumstances, but not all as highlighted by the Privacy International judgment.
- The UK has said it will not incorporate the EU Charter after the transition period ends. Articles 7 and 8 of the EU Charter provide for fundamental privacy rights and data protection rights, which form the basis for the GDPR.

CONCLUSION

The legal parameters around an adequacy decision, the recent legal challenges to existing adequacy decisions, combined with the Judgments will weigh heavily on the Commission when making an adequacy decision in respect of the UK.

The Judgments will have a significant impact on member states, national legislation and businesses in respect of the retention and transmission of data. If you would like any advice on these issues or are uncertain about if they apply to you and your business, please contact John O'Connor or your usual William Fry Contact.

CONTACT

For more information, please contact John O'Connor or your usual William Fry contact.

John O'Connor
PARTNER
Technology
+353 1 639 5183
john.oconnor@williamfry.com

David Cullen
PARTNER
Technology
+353 1 639 5119
david.cullen@williamfry.com

Leo Moore
PARTNER
Technology
+353 1 639 5152
leo.moore@williamfry.com