CJEU Judgement: Dynamic IP Addresses Constitute Personal Data

On October 19, 2016, the Court of Justice of the European Union (CJEU) decided that the dynamic IP address of a website visitor is “personal data” under Directive 95/46EC (Data Protection Directive) in the hands of a website operator that has the means to compel an internet service provider to identify an individual based on the IP address.

The case was brought by Patrick Breyer, a German Pirate Party politician. Breyer asserted that the German government’s storage of IP addresses of users visiting German government websites allowed the creation of user profiles and, therefore, was impermissible under Section 15 of the German Telemedia Act (TMA). In relevant part, the TMA restricts telemedia service providers’ collection and use of users’ personal data except to the extent “necessary to enable and invoice the use of telemedia (data on usage)”. In response, the German government argued that dynamic IP addresses (as opposed to static IP addresses) are not personal data and, accordingly, the government’s storage of dynamic IP addresses Section 15 of the German TMA does not apply.

The CJEU sided with Breyer. The Court largely followed the opinion that the court’s Advocate General issued on May 12, 2016, and which we have previously discussed on our blog. The CJEU relied on the Recital 26 of the Data Protection Directive, which states that in determining whether a person is identifiable, “account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.”

The CJEU found that this test did not limit the scope of information that might be available to the controller to that in the controller’s possession. Instead, the test required the Court to consider data which the controller may “reasonably likely” access and use, and combine with the information in the controller’s possession to identify an individual.

The Court went on to explain that data would not be viewed as “reasonably” accessible to a controller “if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.”

In applying the test to the German government’s program, the Court found that the website operators were collecting the IP addresses to identify cyber attackers and, in some cases, to bring criminal proceedings against them. In this context, the government would likely have a legitimate reason to demand that the internet service provider correlate the IP address to the account holder, and thus allow the government to re-identify the individual. Therefore, the court held that the reasonable likelihood test was met, concluding that the dynamic IP addresses in these circumstances were personal data.

In addition, the Court found (in accordance with its decision in ASNEF and FECEMD) that Section 15 of the German TMA does not comply with the Data Protection Directive because the Data Protection Directive sets out an exhaustive and restrictive list of circumstances in which the processing of personal data can be regarded as being lawful based on the principle of ensuring an equivalent level of data protection in all Member States. Consequently, Member States cannot add new principles relating to the lawfulness of the processing of personal data to Article 7 of the Data Protection Directive or impose additional requirements that have the effect of amending (in particular, limiting) the scope of the six principles provided for in Article 7. According to the Court, Article 7 prohibited controllers from storing personal data (the IP addresses) in absolute terms, and therefore operated as an amendment to Article 7. The Court reasoned that the controller has legitimate interests which might prevail over those of the data subject, and therefore Section 15 of the German TMA offends the competing principle of the free movement of data. In short, the provision is too strict.
Our Take

- It is no surprise that the court found dynamic IP addresses to be personal data in these circumstances given the German government’s intent to use the IP addresses to bring criminal proceedings. However, when dynamic IP addresses or other indirect identifiers become personal data in circumstances where there is no realistic intent or motive to re-associate, but re-association is still possible, it is harder to tell if the test is now whether identification is a “practical impossibility because it requires disproportionate effort”.

- Confirmation of the position that Member State law cannot restrict processing that is quite clearly permitted under the Data Protection Directive should be of much greater comfort to data controllers, but given that it will require a ruling that domestic legislation is invalid is only likely to be an argument advanced as a last resort. Of more immediate relevance, this decision is a warning sign to Member States not to enact rules that restrict the processing of personal data beyond the requirements of the GDPR, except where the GDPR expressly permits Member States to do so.