Client Alert | Data, Privacy & Cyber Security / Technology

IP addresses may be subject to EU data protection laws

May 2016

Authors: **Martin Munz**, **Tim Hickman**, **Matthias Goetz**, **Audrey Oh**

In an ongoing case before the Court of Justice of the European Union ("CJEU"), the Advocate General has issued his Opinion stating that, under certain circumstances, dynamic IP addresses can be "personal data". Businesses that process IP addresses should take note, as their business activities could be adversely affected by EU data protection law if the CJEU follows the Advocate General's Opinion.

On 12 May 2016, Advocate General Campos Sanchez-Bordona (the "**AG**") issued an Opinion in Case 582/14 – *Patrick Breyer v Germany*. The Opinion, which is a standard stage of the CJEU's judicial process, is not yet available in English. The CJEU is not bound to follow the AG's Opinion, although it often does so. A final decision from the CJEU is expected shortly.

The AG's Opinion is significant from a business perspective because, if the CJEU follows the AG's Opinion, businesses will need to ensure that the collection and further processing of dynamic IP addresses is compliant with EU data protection law. This has clear knock-on consequences for website analytics, online advertising, and so on.

Background

The case involves websites operated by the Federal Republic of Germany (the "**BRD**"). Like many website operators, the BRD records the IP addresses of visitors of its websites. Patrick Breyer (a member of the Pirate Party) sued the BRD, claiming that: (i) IP addresses qualify as personal data under EU data protection law; and (ii) that the BRD would require consent for processing such data. Mr Breyer alleged that the retention of IP addresses by the BDR could enable the BRD to profile users of its websites.

On appeal, the Regional Court of Berlin ruled that IP addresses in the hands of website operators qualify as personal data if a user provides additional details to the website operator (e.g., name, email address, etc.). Both parties subsequently appealed this ruling to the German Federal Court of Justice (the "**BGH**"). The BGH has referred several questions to the CJEU regarding the interpretation of the EU Data Protection Directive 95/46/EC (the "**Directive**") in this context. In particular, the BGH asked the CJEU to determine whether dynamic IP addresses qualify as personal data in the hands of a website operator if a third party (e.g., an internet service provider) holds additional information (e.g., account details) that link those dynamic IP addressed to the identities of individuals.

The AG's Opinion

IP addresses

In his Opinion, the AG points out that BGH's question only refers to dynamic, but not to static IP addresses. Most devices use dynamic IP addresses, which are assigned by an internet service provider each time the device connects to the network. Dynamic IP addresses are only temporarily assigned to a device, and generally change each time the device connects to the network. Ordinarily, a dynamic IP address does not provide a website operator with sufficient information to identify an individual user, unless additional information is also available.

Are dynamic IP addresses personal data?

The question of whether dynamic IP addresses are personal data depends on the interpretation of Article 2(a) of the Directive, which defines the term "personal data". According to Article 2(a), personal data is "*any information relating to an **identified** or **identifiable** natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly* […]". Further analysis of the issue of identifiability is provided by the EU's Article 29 Working Party, in its Opinion 4/2007.

While a dynamic IP address alone may not directly identify an individual, all the parties to the proceedings agreed that, in combination with additional information, a dynamic IP address could facilitate the indirect identification of the user. The question before the CJEU is whether dynamic IP addresses qualify as personal data if the relevant additional information is in the hands of a third party (e.g., an internet service provider). In his Opinion, the AG said that this depends on the understanding of Recital 26 of the Directive, which states that "*to determine 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*".

Interestingly, when the UK implemented the Directive, it specifically limited its definition of personal data to information that the controller (in this case, the website operator) holds, or information that "*is likely to come into the possession of*" the controller. However, many other EU Member States (including Germany) did not include the same restriction when implementing the Directive. The AG concluded that "*likely reasonably*" does not mean the website operator that holds the IP address must actually request further information from the third party who holds the additional information. Rather, the AG took the view that the mere possibility that such a request could be made is sufficient (cf. the UK position, noted above).

In short, the AG found that dynamic IP addresses are personal data in the hands of a website operator if an internet service provider has further information, which, in combination with the dynamic IP address, could identify a user, since it was likely reasonable to use the information available at the internet service provider. The questions of: (i) whether the controller (website operator) intended to (or was likely to) attempt to obtain the additional information needed to identify the data subject; and (ii) whether the internet service provider was prohibited by law from disclosing such information to the controller; did not affect this analysis.

Conclusion

The present case expands upon the CJEU's previous ruling in *Case C-70/10 – Scarlet Extended*, in which it was held that IP addresses constitute personal data because they allow users to be identified. However, in that case the facts were different in that the IP address was collected and stored by an internet service provider itself. Moreover, the decision in *Scarlet* only touched on the IP address question as a secondary issue in the context of copyright infringement and the protection of intellectual property rights.

The recently adopted EU General Data Protection Regulation ("**GDPR**") acknowledges that online identifiers (a term which is not further defined in the GDPR, but which appears sufficiently broad to include IP addresses) may be used to identify individuals, and could enable website operators to identify, and create profiles of, those individuals. However, the GDPR does not address the question of what happens if such additional information is held by a third party, (e.g. an internet service provider). It will be interesting to see whether the CJEU follows the AG's Opinion. It is likely that the CJEU's decision in this case will affect the interpretation of both the Directive and the GDPR, and therefore it is hoped that the CJEU will provide clarity on this issue.

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000