European Court of Justice: IP Addresses Are Personal Information

By Alex van der Wolk, Esq., and Hanno Timner, Esq.
Morrison & Foerster

On October 19, 2016, the European Court of Justice ("ECJ" or the “Court”) held that dynamic internet protocol (“IP”) addresses collected by an electronic service provider (e.g., website owners) qualify as personal information under EU privacy laws (Breyer v. Germany, Case C-582/14).

The Court’s ruling means that websites that use visitors’ IP addresses, for instance, to analyze the use of their website (analytics) or for online marketing purposes (such as device fingerprinting or other forms of retargeting), could now be required to first obtain the user’s consent (unless another legal basis is applicable).

However, the ruling can also have implications for companies’ use of key-coded or de-identified data, even if a company itself does not hold the key necessary to re-identify individuals or would need to obtain such a key in legal proceedings through a court order.

If it is possible to indirectly relate key-coded or de-identified information back to an identified person, companies could be required to treat such information as personal information, for which a legal basis needs to be secured.

In the case before the Court, a German politician sought to enjoin the German Federal Government from storing IP addresses of users visiting German public institutions’ websites. The referring court (the German Supreme Court, Bundesgerichtshof) referred two questions to the ECJ for a preliminary ruling:

1. Does a dynamic IP address, which a website is not directly able to relate to an identified user, qualify as personal information; and
2. May local law set restrictions on a company’s ability to use such an IP address on the basis of the legal basis of “legitimate interest”?

THE FIRST REFERRING QUESTION — PERSONAL INFORMATION

The ECJ held that, although a website owner typically cannot directly identify users by their IP addresses, the user’s Internet access provider, which enables the user’s access to Internet and assigns the IP address to the user, is able to relate the IP address to an identified user.

The Court took into account that the electronic service provider cannot directly identify its users based on dynamic IP addresses, because (i) the dynamic IP address is assigned to a user by the Internet access providers, not by the electronic service provider; (ii) the IP address is only unique to the user for as long as the Internet connection is active and reassigned to another internet user, thereafter; and (iii) only the telecom company has the information linking the dynamic IP address to the Internet user.
The Court reasoned that if a website owner wanted to obtain the identity of a visitor (e.g., in case of a cyber-attack), it would be able to do so via that Internet access provider — through a court order if needed. For that reason, the Court held that IP addresses can be used to indirectly identify a user and, therefore, qualify as “personal information” under applicable data protection laws.

This is significant because the ECJ has now formally held that if anyone has the ability to identify the individual indirectly (even if it is a different company that has the key and a court order would be required), the de-identified or key information could still qualify as personal information.

**THE SECOND REFERRING QUESTION — LEGITIMATE INTEREST**

The second referring question arose because German law (the Telemedia Act) places limitations on websites to collect personal information. The law provides that websites may only collect personal information without the users’ consent if this is necessary to provide or invoice their service. The German government’s use of IP addresses did not fall under these authorized uses described in the Telemedia Act.

The ECJ held that the German Telemedia Act unduly limits companies’ use of their “legitimate interest” ground (Art. 7 of the EU Privacy Directive 95/46). The Court indicated that, in addition to providing or invoicing for services, there could very well be other purposes of a website’s use of personal information that are within the website’s legitimate interest.

The German Telemedia Act, however, does not allow those other purposes. As a result, it limits the scope of Art 7 of the Directive, which the Court held is not permitted; Member states are precluded from imposing additional requirements on any of the principles provided for in Art. 7 of the Directive.

This is also important because the ECJ has now said that laws that place undue burden on an organization’s ability to use the legitimate interest ground as a basis for legitimizing the collection and use of personal information are not permitted.

**IMPLICATIONS FOR BUSINESS**

Electronic service providers/website operators will no longer be able to argue that IP addresses are anonymous information. Therefore, where collecting and storing the IP addresses is not essential to providing the services, organizations may now be required to obtain user consent or being able to legitimate the use based on a specific legitimate interest (e.g., security or allowing the website to operate).

It should be noted that, under the GDPR, electronic service providers will have to specifically inform users of what that legitimate interest is, and they will need to be able to account for the collection of IP addresses, as well as key coded information, including the need to articulate the legal basis of such data processing.

The case will further impact the controversy around key coding and anonymization more generally. Some Member States consider that information is anonymous when the holder of the key coded information cannot re-identify it, even if a third party has the key. Other Member States take the view that as long as someone can re-identify the information, it remains personal information.

The ECJ’s findings clearly back up this second approach and will make it very difficult, if not impossible, to maintain the view that key-coded information does not qualify as personal information so long as the key exists.

The case may be especially important for electronic service providers involved in connected devices in the Internet of Things. The extension of the IP address pool (IPv4 to IPv6) is set to vastly expand the number of available IP addresses. Combined with the rise of “smart” technology in every day appliances, technologists expect that in the future, most man-made objects will have some type of Internet connectivity, each with a unique IP address.
If these devices were to communicate remotely with electronic service providers, such communication would likely expose the IP address to the electronic service provider and thereby trigger data protection rules (which, again, will typically mean user consent or, at least, express notice as to the processing, backed up by a legitimate interest).

This decision is also very important for companies involved in medical and drug research, or in the pharmaceutical industry, which relies in large part on using key-coded data.

The decision of the ECJ confirms the opinion of the Advocate General in May 2016.