IP Addresses Fall Under EU Privacy Law, Top Court Says

Decision at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1034974

By Allison Grande
Law360, New York (October 19, 2016, 11:12 PM EDT) -- Europe's highest court ruled Wednesday that dynamic internet protocol addresses that require help from service providers to link to individuals can be considered personal information under the bloc's current data protection regime, although it found that websites are free to collect such data in order to combat cyberattacks.

The European Court of Justice's two-part ruling stems from a dispute over the scope of the bloc's 1995 general data protection directive that was launched by German activist Patrick Breyer, who asserted that the government's collection and storage of his dynamic IP address when he visited various websites operated by federal agencies ran afoul of the law.

In referring the matter to the high court in 2014, Germany's Federal Court of Justice asked whether dynamic IP addresses that websites collect from their visitors but can't be tied to those individuals without the assistance of an internet service provider fell within the definition of personal data under Article 2(a) of the directive, and whether member states in implementing the directive into their national laws could restrict website operators from lawfully collecting the data for the purpose of securing their websites against cyberattacks.

In answering the first question, the Court of Justice concluded that because the directive defines personal data as information that can be used to identify a person either "directly or indirectly," dynamic IP addresses — which unlike static IP addresses are only temporarily assigned to users by their ISPs when they start a new browsing session and are not continuously linked to their device — do fall under the directive.

"The use by the EU legislature of the word 'indirectly' suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified," the court ruled. "The fact that the additional data necessary to identify the user of a website are held not by the online media services provider, but by that user's internet service provider does not appear to be such as to exclude that dynamic IP addresses registered by the online media services provider constitute personal data within the meaning of Article 2(a) of [the] directive."

The high court noted that it had previously found in a 2011 decision that IP addresses collected by ISPs were protected personal data under the directive because they could be used to identify users precisely. But while the matter raised by Breyer involved

collection and retention of IP addresses by online service providers who do not have the information that ISPs have to identify users, the high court still concluded that this data should be given the same treatment because website operators have legal means to get that information from service providers, particularly in instances where the operator needs to identify the source of an IP address that may be causing harm to its site.

"In the event of cyberattacks, legal channels exist so that the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider and to bring criminal proceedings," the ruling said. "Thus, it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons ... on the basis of the IP addresses stored."

The subject of what website operators are allowed to do when it comes to securing their websites also came up in the high court's consideration of the second question, which dealt with how far member states like Germany could go in restricting for what purposes processors can use data for without obtaining consumers' consent.

Under Section 7(f) of the directive — which in May 2018 will be replaced with a more stringent and uniform general data protection regulation — website operators are allowed to process personal data in instances where the "legitimate interests" of the operator is not overridden by the "fundamental rights and freedoms" of the data subject.

In implementing the directive into its national law, Germany limited this processing to only personal data that is "necessary to facilitate and charge for the use" of a site's services. But the European Court of Justice found that this interpretation was too narrow because it would prevent website operators from storing IP addresses for other legitimate and important purposes, including being able to identify and combat those who carry out "denial of service" attacks that paralyze sites by flooding web servers with traffic.

"Member states cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case," the ruling said. "Such a restrictive reading of [German law] would prevent the storage of IP addresses from being authorized in order to guarantee in a general manner the security and continued proper functioning of online media."

In a statement Wednesday, Breyer expressed concern with the court's refusal to block website operators from surreptitiously collecting IP addresses to combat cyberattacks.

"Internet companies will still follow us around the web, collect information about our

private interests and pass this information on," Breyer said. "Now the EU has to close this unacceptable loophole in data privacy laws as quickly as possible."

The case is Patrick Breyer v. Bundesrepublik Deutschland, case number C−582/14, in the Court of Justice of the European Union.

--Editing by Mark Lebetkin.