

Take 2: Personal data and dynamic IPs – time for clarity?




Damian Clifford and Jessica Schroers, legal researchers at KU Leuven, look at whether dynamic IP addresses fall within the scope of European Data Protection legislation given the identifiability of users based on the processing of IP addresses. In this post, they examine the written submissions and the hearing of the the Court of Justice of the European Union (CJEU) which provide some direction on whether dynamic IP addresses can be interpreted as personal data.

In our [previous blogpost](#), we examined a reference from the German Federal Court of Justice (*Bundesgerichtshof*) to the Court of Justice of the European Union for a preliminary ruling on the status of dynamic IP addresses as personal data under [Directive 95/46/EC](#). This preliminary ruling could provide clarity in relation to the application of the EU Data Protection Framework to the collection of IP addresses and hence the strict legal requirements contained therein. The purpose of this post is to provide an update on the case following the submission of written opinions and the public hearing that was held on 25 February 2016. In simple terms, IP addresses are unique sets of numbers that identify each computer using the Internet Protocol system to communicate over a network. However, IP addresses can be either static or dynamic. The latter refers to situations in which a new address is assigned to each computer every time it connects to the internet. In contrast, static IP addresses remain attached to the same computer.

[The first question](#) referred by German Court to the CJEU relates to whether the classification of IP addresses as personal data also extends to dynamic IP addresses in situations where the website operator who processes the IP addresses does not have the identifying information necessary to link them to individual users. In such cases, the identifying information is instead held by a third party (i.e. the ISP) and is therefore beyond the reach of the website operator without direct cooperation between the parties. [The second question](#) focuses on whether §15 of the German Telemedia Act is legitimate in light of Directive 95/46/EC and hence whether the grounds for processing contained in Article 7(f) can be relied upon for the collection of IP addresses in order to ensure the functionality of a website. Article 7(f) states that processing is only allowed if it is necessary for the purposes of a legitimate interest pursued by the controller and is not overridden by the interests and fundamental rights of the data subject (i.e. the user).

During the hearing, much of the Court's focus was on the second question and, more specifically, on the interpretation of 'legitimate interests' in Article 7(f) Directive 95/46/EC and the role of the national courts. The applicant, Mr Breyer, argued that whilst he had used various German state websites (which had stored data including dynamic IP addresses), he had not given his consent for the data to be processed. Although Breyer's legal representative argued that ensuring the proper functioning of a website does not fall within the scope of Article 7(f), there appeared to be a general consensus that the balancing exercise at the core of this question (i.e. regarding the proportionality of the gathering vis-à-vis the security of the website) is a matter for the national Court. There were, however, divergent views on the first question which presents an important debate in the application of the Directive's definition of personal data.

The substantive sticking point

The key to the first question rests on the interpretation of the provisions in Directive [95/46/EC](#) which cover the scope of the definition of personal data. 

Article 2(a) of Directive 95/46/EC defines ‘personal data’ as:

“any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, [...]”

In addition, recital 26 of Directive 95/46/EC provides further clarification:

“[...]whereas, 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; [...]”

The statements submitted prior to the hearing by Member States indicate a fundamental division on the classification of dynamic IP addresses, which is unsurprising given the **differing national approaches to this issues**.

Contentious interpretations

Germany argues that dynamic IP addresses do not constitute personal data if the information necessary to identify the user is in the hand of a third party. In contrast, the others who submitted opinions (i.e. the applicant (Breyer), Austria, Portugal and the European Commission) interpret dynamic IP addresses as personal data.

Germany adopts a relative approach in relation to identifiability and argues that, due to the wording of Article 2(a) and recital 26, only the means that are ‘likely reasonably to be used’ should be taken into account. In simple terms, Germany argues that the determination of whether something is reasonable depends on the technical and legal hurdles in addition to the effort (e.g. with regard to time, money and/or manpower) that is required. If the effort is disproportionate, the means should not be considered reasonable. Austria, Portugal and the European Commission however interpret Article 2(a) as only requiring a person to be identifiable. For them, recital 26 clearly explains that identifiability encompasses all the means likely reasonably to be used by any other party and that therefore dynamic IP addresses constitute personal data.

The main discussion point is therefore what can be considered as ‘means likely reasonably to be used’. Germany argues (in reference to the opinion of its Federal Court of Justice) that ISPs are only allowed to provide data to third parties (here, the website operator) if the law specifically permits such transfers, or when the data subject has consented to it. As such, if there is no legal basis for providing the information to a third party, the website operator would not gain access to the data. The key to this argument is that whilst some offices (such as the prosecutor in preliminary legal proceedings) may gain access to such data, this does not mean that every office of the Federal Republic of Germany has access.

Portugal and the European Commission make clear that they deem the obtaining of information from ISPs as ‘likely reasonably’. Considering that Germany justifies the logging of IP addresses as a security measure and that the act of logging does not itself prevent attacks, the effectiveness of this measure is linked to the fact that individuals who for instance attempt to hack the website can then be retrospectively identified through the IP address. Thus, if the reason for logging IP addresses is to be able to identify individuals if necessary, such means should not be considered unreasonable. During his oral submission, Breyer’s legal representative expressed a similar opinion by referencing the fact that several thousand information requests to reveal the identities behind IP addresses are made per year. Consequently, it was argued that if Germany’s position on this issue were maintained, the legal protection of data subjects would be severely hampered as there would be too much flexibility and the protection would be diluted, a point which appeared to be supported by the Commission at the hearing.

CJEU: an opportunity to clarify the situation?



In essence, the key point is whether or not obtaining identifying information from an access provider can be interpreted as ‘likely reasonably’. It is hoped that the Court’s decision will provide more certainty in relation to this question. The case presents the CJEU with the opportunity to clarify the status of dynamic IP addresses as personal data and to interpret this issue in line with the Article 29 Working Party which would harmonise interpretations across the EU. Indeed, the inability to distinguish between static and dynamic IPs has proven to be a key issue in the classification of such identifiers as personal data.

However, the judgement may alternatively focus on the purpose for which Germany gathered the IP addresses instead of deciding on the potential differentiation between static and dynamic IPs in a broad and more general manner, thereby limiting the judgement to a purpose-based reasoning. Indeed this appears to be the likely outcome, given the focus of the questions and arguments made at the hearing. Such an approach would therefore leave the national German Court to decide whether the security interests of the website operator outweigh the privacy interest of the internet user. More insights into the possible interpretation of this issue by the Court will be revealed in the Advocate General’s opinion, due on 12 May 2016.

This article gives the views of the authors, and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics and Political Science.

This work was partly funded by the European Union FP7 project ECOSSIAN (607577). Damian Clifford’s research for this blog is funded by The Research Foundation – Flanders (FWO) – (FWO Aspirant) KU Leuven Centre for IT and IP Law.

March 4th, 2016 | [EU Media Policy](#), [Featured](#), [Internet Governance](#) | [1 Comment](#)

⤴

