IP addresses and personal data: Did CJEU ask the right questions?

The Court of Justice of the European Union has declared that IP addresses are personal data in many circumstances – but were the right questions asked, and will the GDPR change the outcome? By **Tim Hickman**, **Matthias Goetz**, **Dr Detlev Gabel** and **Chris Ewing**.

On 19 October 2016, the Court of Justice of the European Union (the CJEU) delivered its highly anticipated decision in Case C-582/14 – *Patrick Breyer v Germany* (Breyer), concerning the definition of "personal data" under the EU Data Protection Directive 95/46/EC (the Directive). Article 2(a) of the Directive provides that the term "personal data" means: "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 particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

The Federal Republic of Germany (BRD) operates a number of websites. Like many website operators, the BRD records the IP addresses of visitors to its websites. Patrick Breyer, a visitor to the BRD websites and a Pirate Party politician, sued the BRD, claiming that his IP address, which had been recorded by the BRD's websites, constitutes his personal data.

The parties in *Breyer* agreed that the IP address data did not directly identify Mr Breyer. Mr Breyer nevertheless argued that his IP address was his personal data, because information held by his Internet Service Provider (ISP) could be used to link the BRD's IP address records to Mr Breyer's real world identity (i.e., although the BRD could not directly identify Mr Breyer from his IP address, the BRD could indirectly identify him from the combination of his IP address and the records held by his ISP).

> The CJEU accepted that there could be cases in which IP addresses would not necessarily be personal data

On the facts, the CJEU held (at paragraph 73 of Breyer) that:

(i) there was a "*practical possibility*" that the BRD could obtain the necessary information from Mr Breyer's ISP;

(ii) that such information could be obtained "*within the framework of the law*"; and

(iii) that it was therefore "*reasonable*" to suppose that the BRD could identify Mr Breyer. "

Accordingly, the IP address, in the hands of the BRD, was held to be personal data. It should be noted that the CJEU accepted that there could be cases in which IP addresses would not necessarily be personal data (e.g., where it is illegal, or practically impossible for reasons of time, effort or expense, to identify the individual) although it seems likely that these cases are the exception, rather than the norm.

But did the CJEU ask all of the right questions in *Breyer*? The judgment discusses the question of whether it was possible for the BRD to obtain Mr Breyer's real-world identity, but does not discuss the question of whether the BRD was likely to try to identify Mr Breyer, which is very different test. While it appears that the BRD reasonably could have identified Mr Breyer from his IP address had it wished to do so, there was no evidence at all that the BRD was likely to attempt to do so.

A question of translation

In the English translation of the Directive, Recital 26 states: "to determine whether a person is identifiable, account should be taken of all means *likely reasonably* to be used either by the controller or by any other person to identify the said person" (emphasis added).

The French translation contains similar wording (*susceptibles d'être raisonnablement*). As set out above, the CJEU did not consider the question of whether the BRD held means which were likely to be used to try to identify Mr Breyer, which initially appears to be inconsistent with the language in the English and French translations of Recital 26 to the Directive. However, several other translations of Recital 26 to the Directive do not refer to the concept of likelihood. For example, the German translation uses the term "reasonably" (*vernünftigerweise*) but does not use a term for "likely". Similarly, the Dutch translation uses the term "reasonably" (*redelijkerwijs*) but includes no term for "likely". Consequently, the CJEU's analysis in *Breyer* (which addresses the term "reasonably" but not the term "likely") appears to be consistent with some translations of the Directive, but not others. Curiously, the CJEU judges in Breyer appear to have predominantly come from EU Member States whose national language translations of Recital 26 to the Directive do not include a word for "likely".

Conflicts between different translations of the Directive have arisen before. For example, in its Opinion 8/2010, the Article 29 Working Party (WP29) noted (on page 20 of that Opinion) that the English translation of Article 4(1)(c) of the Directive uses the word "equipment". The WP29 considered that this term was too narrow. Instead, the WP29 opined that the correct term would be a "means" of processing (encompassing any method by which personal data are processed, whether or not "equipment" is used).

However, that conflict of translations was fairly trivial, and the WP29's Opinion (while not legally binding) was generally accepted to be correct by most practitioners. The conflict of translations that arises in relation to Recital 26 to the Directive, and the CJEU's analysis in Breyer, is far less clear-cut.

'Likelihood' and the national laws of EU Member States

The language of the English translation of recital 26 to the Directive was also implemented into the UK via the Data Protection Act 1998 (the Act). Section 1(1) of the Act states that "personal data" means: "data which relate to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, *or is likely to come into* the possession of, the data controller" (emphasis added).

If this definition had been applied to the facts of *Breyer*, the IP address data held by the BRD would not have constituted Mr Breyer's personal data unless Mr Breyer could show that the additional information necessary to link his IP address to his real world identity was likely to come into the possession of the BRD.

On the other hand, the German Federal Data Protection Act (*Bundesdatenschutzgesetz*), like the definition set out in the German translation of the Directive, makes no reference to the concept of likelihood. Notwithstanding the fact that, as noted above, the French translation of Recital 26 to the Directive includes a term for "*likely*" (*susceptibles*), the French Data Protection Act (Act N°78-17 of 6 January 1978, as amended) does not use that term.

It appears that national legal traditions have taken diverging approaches to the question of whether "*likelihood*" forms any part of the definition of personal data. Unfortunately, the CJEU did not address this point in *Breyer* but, as set out below, it may be forced to reconsider the matter in the near future.

Breyer in the light of the GDPR

Enforcement of the General Data Protection Regulation (GDPR) begins on 25 May 2018. Because the GDPR is an EU Regulation it will, from that date, override the national laws of EU Member States, to the extent that those national laws conflict with the provisions of the GDPR.

The GDPR contains a Recital that is very similar to Recital 26 to the Directive – coincidentally also numbered Recital 26. The English translation of Recital 26 to the GDPR states: "to determine whether a natural person is identifiable, account should be taken of all the means *reasonably likely* to be used…" (emphasis added).

This is fairly similar to the language in the English translation of Recital 26 to the Directive, which is perhaps unsurprising. What is more surprising is the fact that the other translations of Recital 26 to the GDPR consistently include a term for "*likely*". For instance, the French translation uses the expression "*reasonably likely*" (*raisonnablement susceptibles*), the German translation uses the term "*likely*" ("*wahrscheinlich*"), and the Dutch translation uses the phrase "reasonably to be expected" ("*redelijkerwijs valt te verwachten*") which, at the very least, seems to imply something more than a mere possibility.

This is obviously problematic. The CJEU clearly stated in *Breyer* that IP addresses are personal data if the website operator is reasonably able to identify the data subject from the IP address and other information that could lawfully be obtained from an ISP – without reference to the concept of likelihood. But many translations of Recital 26 to the GDPR impose a test that requires an analysis of likelihood. It seems that any such test would need to be evidence-based. If Mr Breyer could produce evidence that the BRD was likely to try to identify him (e.g., if he could show that the BRD had requested information about his identity from his ISP) then it appears that the test in Recital 26 to the GDPR would be satisfied (meaning that his IP address would be personal data in the hands of the BRD). Conversely, if Mr Breyer could not show that the BRD was likely to attempt to identify him, then it appears that that test would not be satisfied (meaning that his IP address would not be personal data in the BRD's hands). As a result, serious questions arise as to whether the test set out by the CJEU in *Breyer* will continue to be good law after enforcement of the GDPR begins on 25 May 2018.

Impact on businesses

The CJEU's decision in *Breyer* expands upon its previous decision in Case C-70/10 – *Scarlet Extended* (in which the CJEU held that IP addresses could constitute personal data, but offered very little analysis as to why that was the case). The *Breyer* decision provides much greater clarity on this point, concluding that IP addresses will be personal data wherever the website operator is reasonably able to identify the relevant individuals (e.g., by lawfully obtaining further information from the relevant ISPs). In practice, website operators cannot know in advance which IP addresses they can reasonably link to individuals, and which they cannot. Consequently, website operators will be forced to treat all IP addresses as personal data, and they will therefore have to comply with EU data protection law in respect of the handling of all IP addresses (to the extent that those website operators are subject to the jurisdiction of EU data protection law). This has material consequences for businesses that use many forms of online targeted advertising or cookie tracking, which often relies on the use of IP addresses.

On the other hand, this obligation may be short-lived. From the point at which enforcement of the GDPR begins, website operators will be able to point to the fact that although they might reasonably be able to identify individuals from their IP addresses, they are not likely to do so. Therefore, they may be able to argue that IP addresses in their possession do not constitute personal data for the purposes of the GDPR. How the CJEU will apply the test under the GDPR remains to be seen, and website operators should keep this issue under review.

AUTHORS

Tim Hickman and Matthias Goetz are Associates in the London office of White & Case. Dr Detlev Gabel is a Partner in the Frankfurt office of White & Case and Chris Ewing is a trainee solicitor in the London office of White & Case.
Emails: tim.hickman@whitecase.com
dgabel@whitecase.com
matthias.goetz@whitecase.com