The European Court of Justice case of *Breyer*

Mr. Alan S. Reid
Sheffield Hallam University

Abstract

This case note analyses the impact and significance of the European Court of Justice decision in *Breyer*. The European Court of Justice has expanded the definition of personal data to include dynamic IP addresses. The judgment improves the privacy situation of internet users across the European Union.

The facts of Breyer[1]

Patrick Breyer is a German politician and activist who belongs to the Pirate Party. The Pirate Party was originally set up in Sweden in 2006, as a single issue political party, committed to the modernisation of copyright law in Sweden, following the crackdown on The Pirate Bay peer-to-peer network. After limited success in Sweden, sister parties sprung up across Europe, in order to capitalise on the notoriety of The Pirate Bay. In order to broaden their appeal, the European Pirate Parties set out common themes of campaigning interest, in particular, on issues surrounding the internet, such as open access to information, freedom of expression and privacy. As a technophile and politician committed to internet freedoms, Patrick Breyer vociferously objected to various Federal German government websites retaining details of his dynamic Internet Protocol (IP) address after he had completed browsing.

Internet Protocol (IP) addresses are the essential backbone of the internet. Internet protocols are the method by which interconnected computers and devices communicate, share and transfer data between themselves. An IP address consists of either four pairs of numbers (version 4)[2] separated by three colons or eight pairs of numbers separated by six colons (version 6).[3]

The US organisation ICANN[4], the Internet Corporation for Assigned Names and Numbering, is tasked with overseeing the interconnectivity and compatibility required for the continued successful operation of the internet infrastructure. As part of this regulatory function, ICANN has created a new US corporation, called Public Technical Identifiers (PTI)[5], in order to fulfil the functions assigned by it to the Internet Assigned Numbers Authority (IANA).[6] A significant part of the function of IANA is to coordinate the assignation of IP addresses across the world, via five regional registries.[7] European IP addresses are allocated through the

[1] Case C-582/14 *Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:779.
[2] Version 4 of the IP protocol address system. This system was set up in 1983.
[3] Version 6 of the IP protocol address system. This system became operational in June 2012 on World IPv6 Launch day: http://www.worldipv6launch.org/faq/.
[4] ICANN's website is available at; https://www.icann.org/.
[5] PTI's website is available at; https://pti.icann.org/. PTI began operating in October 2016, a few weeks before the judgment of the ECJ in Breyer.
[6] IANA's website is available at; http://www.iana.org/.
[7] An overview of IANA's functions in relation to IP numbers is available at; http://www.iana.org/numbers.

organisation Réseaux IP Européens (RIPE).[8] RIPE assigns IP addresses to Local Internet Registries (LIR) in each country coming under its jurisdiction. LIRs include Internet Access Providers such as Internet Service Providers (ISPs), general telecommunication providers and large corporations. These LIRs, in turn, then assign their allocated IP addresses to their customers, affiliates and partners.

Internet Protocol addresses can be dynamic or static. A dynamic Internet Protocol address is a temporary identification number given by an internet access provider such as an Internet Service Provider (ISP) to its customers' devices when they are used to connect to the internet.[9] A static IP address, as its name suggests, is a permanent assigned identifier number enabling devices to access the internet. Static IP addresses are more expensive and are more suited to professional, commercial and really heavy industrial users of the internet such as large businesses, universities and government agencies. These organisations require a fixed IP address in order to ensure continuity and reliability of their internet-reliant services such as internal communications, hosting computer servers and maintaining their webpages. Their fixed nature means that identifying the individuals concerned is much easier than when using a dynamic, changing set of numbers allowing access to the internet. The fixed IP address can quite accurately provide the geographical location of the device being used to connect to the internet. In such circumstances, the IP address can become personally identifiable information, that is protected by EU privacy and data protection law.

Internet Service Providers (ISPs) prefer to provide their customers with dynamic IP addresses simply because they are cheaper to provide since the numbers can be recycled and re-used. Further, because residential and small scale users of the internet, their family and their guests will be using a number of internet-enabled devices to connect to the internet at the same time, each device will require a separate IP address.

The dynamic IP address, in contradistinction to the static IP address, only provides limited information about the user of the internet-enabled device. The dynamic IP address can identify the device being used to connect to the internet but on its own does not provide any further identifying details. In most cases, these dynamic IP addresses cannot identify the user of the internet connected device since after the connection is terminated, the IP address is also forgotten. However, in certain cases, this 'agnostic' information can become personally identifiable information when it is combined with other parcels of information. In the case of ISPs, the ISP will be able to easily personally identify their customers for billing purposes and for assisting in the investigation, detection and prosecution of serious crime.[10]

In the example of the ISP outlined above, there is no doubt that the dynamic IP address is personally identifiable information protected by EU data protection and privacy law. In the hands of the ISP, a dynamic IP address is easily combinable with other data held by the ISP to personally identify individuals. By way of example, in a family home, if the ISP also offers contracts to the family for internet-enabled devices such as tablets and mobile phones, when

[8] RIPE's website is available at; https://www.ripe.net/. RIPE is also responsible for allocating IP addresses in the Middle East and certain countries of Central Asia.

[9] Opinion of Advocate General Campos Sanchez-Bordona in Case C-582/14 *Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:339, at para. 1.

[10] Opinion of Advocate General Campos Sanchez-Bordona in Case C-582/14 *Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:339, at para. 2, citing the terms of the EU Data Retention Directive, Directive 2006/24/EC.

those devices are connected to the primary internet account via Wi-Fi, then the ISP will know which member of the family used which device to connect to the internet.

This legal position was settled by the European Court of Justice in its earlier jurisprudence in *Scarlett Extended*[11] and fully accords with both the purposive interpretation of article 2(a) and recital 26 of the Data Protection Directive[12] and the progressive view of dynamic IP addresses by the Article 29 Working Party on Data Protection.[13]

Article 2(a) of the Data Protection Directive provides the definitive definition of 'personal data' in the EU legal space. Personal data is data that relates to an identified or 'identifiable' natural person. An identifiable person is a person who can potentially be identified directly or indirectly by an identification number.

Opinion 4/2007 of the Article 29 Working Party on the concept of personal data[14] considers that dynamic IP addresses can readily be classified as personal data since this information can easily be combined with the other 'log' data collected by the Internet Access Provider or manager of the Local Area Network (LAN) such as the date, time and duration of the internet access in order to precisely identify the actual person using the internet.

Recital 26 of the Data Protection directive states that when determining whether a person is identifiable from information, 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.'

In *Scarlett*, the European Court of Justice decided that Scarlett, a Belgian ISP did not have to install filtering and blocking software which would enable it to identify its customers who were illegally downloading, sharing and uploading copyrighted material and thereafter prevent its customers from committing future transgressions of Belgian and European intellectual property law. In part, the European Court of Justice held that such a system would involve the widespread and systematic collection of IP addresses by Scarlett which would enable the company to precisely identify its customers.[15] Such personally identifying data is protected by the relevant provisions of the EU's Charter of Fundamental Rights[16], general EU data protection law and the terms of specific data protection laws such as the e-Privacy Directive.

---

[11] Case 70/10 *Scarlet Extended v SABAM*, ECLI:EU:C:2011:771.
[12] Directive 95/46/EC.
[13] Article 29 Working Party comprises representatives of the national data protection authorities across the EU, the European Data Protection Supervisor and the European Commission.
[14] See in particular, pages 16 and 17 of Opinion 4/2007. The Opinion is available at; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. This Opinion directly draws on the views of the Working Party from 2000. See *WP 37: Privacy on the Internet - An integrated EU Approach to On-line Data Protection*- adopted on 21.11.2000, available at; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf.
[15] Case 70/10 *Scarlet Extended v SABAM*, at para. 51.
[16] Article 8 of the Charter provides for the right to protection of personal data and article 11 guarantees the right to freedom of expression, which explicitly includes the right to receive and impart information. The text of the Charter is available at; http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

The Legal Impact of Breyer

The *Breyer* case is significant because it clarified and extended the application of the 'identifiability' test expressed in the Data Protection Directive and is part of a wider recognition of the problems associated with modern e-communications.

In Patrick Breyer's case, the factual matrix and actors involved were quite different from those of Scarlett. In the case of Breyer, Patrick Breyer was accessing websites of the federal German government. The federal German government, in its private capacity as a website host, was maintaining a log of dynamic IP addresses of people who had visited its websites, with the explicit aim of fighting the threat of cybercrime, in particular the risk of the website succumbing to a Distributed Denial of Service[17] (DDOS) attack which would disable the website.

In this type of case, the dynamic IP address does not readily relate to personally identifiable data. The holder of the dynamic IP address information is not the ISP but the actual website operator. The website operator does not possess any extra information which can be used in conjunction with the dynamic IP address to identify the specific internet user. In such circumstances it was unclear as to whether a dynamic IP address could be classified as being personally identifying data.

In light of this inherent ambiguity, the German Federal Court of Justice, hearing the dispute between the Federal Government and Mr. Breyer, had no option but to seek interpretative guidance from the European Court of Justice, via the Preliminary Ruling procedure.[18]

Upon receipt of the request from the German court, the European Court of Justice was faced with a binary choice between an 'objective' or 'relative' interpretation of the notion as to whether a person is identifiable or not from their dynamic IP address.[19] The prevailing legal orthodoxy was that such information would only be personal data capable of identifying a person where that information was in the hands of the Internet Service Provider, as was the case in *Scarlett.*[20] In particular, dynamic IP addresses would not be personally identifying information in the hands of the operator of an internet café offering free Wi-Fi.[21] Therefore, under EU law, dynamic IP addresses would only be personal data according to a 'situational' occurrence, when the Internet Access or Service Provider possessed additional information transforming the dynamic IP address into a personal identifier.

Thus, dynamic IP addresses were subjectively defined as constituting personal data. An objective view would have the advantage of being more predictable and certain, however, to do so would unjustifiably greatly expand the reach of EU data protection law. Dynamic IP addresses only transmogrify into personal data when conjoined with other personally identifying data. However, were the European Court of Justice to simply confirm the earlier jurisprudence of *Scarlett*, dynamic IP addresses would only transmogrify into personal data

[17] The online Oxford Living English Dictionary defines a Distributed Denial of Service Attack as 'The intentional paralysing of a computer network by flooding it with data sent simultaneously from many individual computers'. https://en.oxforddictionaries.com/definition/distributed_denial_of_service.
[18] The provisions of the Preliminary Ruling procedure are set out in article 267 of the Treaty on the Functioning of the European Union (TFEU).
[19] See, in particular, the discussion of the ECJ in *Breyer* at para. 25.
[20] See for example, the discussion of *Scarlett* by A-G Campos Sanchez-Bordona in *Breyer*, at para 6.
[21] See Opinion 4/2007 of the Article 29 Working Party, at page 17.

in a small number of specific circumstances related to ISPs. Such a continued restrictive interpretation of the circumstances in which dynamic IP addresses would transform into personal data would fatally undermine the scope and application of EU data protection and privacy law in the uber-Orwellian modern world of global communication networks.

In the era of e-communications after the revelations of Edward Snowden[22] concerning the alleged mass surveillance of millions of people by the US National Security Agency (NSA), netizens[23] are rightly concerned about the power of national intelligence agencies to intercept, read and listen to their online communications. Indeed the blanket, indiscriminate and routine retention of traffic and location data in the EU, such as IP address data, as authorised by the Data Retention Directive was declared illegal by the European Court of Justice in its seminal case of *Digital Rights Ireland*, in 2014.[24] Further, the European Court of Justice, more recently in December 2016, in the joined cases of *Tele2*[25] and *Watson*[26], declared that Swedish and UK domestic law authorising the general retention of communications data, including IP addresses, was incompatible with the EU E-privacy Directive, Directive 2002/58. The European Court of Justice considered that IP addresses should only be retained for the purposes of detecting, prosecuting and investigating serious crimes. Additionally, such retention must be done in a targeted and specific way. This privacy-enhancing judgment of the European Court was only made possible by its earlier reasoning in *Breyer*.

The ambiguity inherent in *Breyer* was resolved by the European Court of Justice in a privacy-enhancing manner. The European Court of Justice rejected calls for a more objective definition of dynamic IP addresses, preferring to clarify the current relative definition offered in *Scarlett*. The court declared that dynamic IP addresses constitute personal data when the provider of a website has legal means available to it to access the additional identifying data held by the relevant ISP.

The court's justification[27] for its stance, as stated earlier, is based on the expansive scope of article 2(a) of the Data Protection Directive, which provides that an identifiable person is someone who can be identified directly or 'indirectly'. In assessing the indirect identifiability of a person, the court focussed on the terms of recital 26 of the Directive, which states that in determining the identifiability of a person, account should be taken of the means likely reasonably to be used by the controller or any other person to identify.

This judicial definition of identifiability expands the scope of personal data protection beyond the limited factual position of *Scarlett*, but falls short of becoming an objective test that would subvert the entire distinction between personal data and non-personal data. Rather, the court has chartered a clear course through this legal minefield and has provided a more workable definition that bears more relation to reality. Dynamic IP addresses only become personally identifying information in certain circumstances. Those circumstances have been clarified by the court in *Breyer*. Dynamic IP addresses will not be personal data when the

[22] Edward Snowden was a contractor for the US National Security Agency who disclosed various documents about the NSA's activities to the Guardian journalist Glenn Greenwald. Details of the contents of these released files are available on The Guardian newspaper's online portal, available at; https://www.theguardian.com/us-news/the-nsa-files.

[23] Netizen is a portmanteau that refers to a Citizen of the Internet, who uses the internet in a reasonable and proper manner. See for example, https://en.oxforddictionaries.com/definition/netizen

[24] Case C-293/12 *Digital Rights Ireland* ECLI:EU:C:2014:238.

[25] Case C-203/15 *Tele 2 Sverige AB* ECLI:EU:C:2016:970.

[26] Case 698/15 *Secretary of State for the Home Department* v *Watson* ECLI:EU:C:2016:970.

[27] See para 41 of the judgment.

linking of the IP address with the other data enabling identification is prohibited by law or when that data can only be acquired using disproportionate means in terms of time, cost or human resources.[28]

Beyond *Breyer*

This incremental, progressive interpretative approach of the European Court of Justice has merit because it offers a logical extension of the law and is consonant with the direction of travel of EU privacy law.

The EU legislature finally approved the new General Data Protection Regulation in April 2016,[29] the European Commission having originally commenced a systematic overview of the data protection directive in November 2010.[30] The terms of this Regulation will apply from the 25th of May 2018.[31] Under the terms of this Regulation, the notion of 'personal data' is extended to specifically encapsulate pseudonymised data, that is data which could be combined with other data to thereafter identify an individual.[32] Further, recital 30 of the Regulation, confirms the EU view that IP addresses are online identifiers.

Thus, under these new legal provisions, website operators and other data controllers will have to ensure that they fully comply with the data protection rules. Effectively, website operators will have to ensure that users of their website are made fully aware of the uses made of their IP address, including who is entitled to gain access to that information and to whom these details will be forwarded. The new rules mean that website operators will need to treat IP addresses in the same way as they do with cookies, that is the small files that are placed on the users' device when they visit a website. The European Court of Justice, in its *Breyer* decision, has arguably given effect to the tenor of the General Data Protection Regulation eighteen months early.

The Court, in rendering its judgment, was also cognisant of developments in the availability and accessibility of the internet across Europe. It has been consistently held in the past that IP addresses are not personal data in the case of internet cafes, since their *raison d'etre* is to offer a space for anonymous web browsing.[33] However, the availability of entirely anonymous spaces for web browsing may be coming under attack as a result of other jurisprudence emanating from Luxembourg.

The case of *McFadden v Sony Music*[34] saw the European Court of Justice confront the issue of copyright violations being committed over unsecured free Wi-Fi provided by commercial organisations to their customers. Mr McFadden was taken to court for 'indirect' copyright violation on the basis that he had failed to secure his Wi-Fi by means of password protection.

---

[28] See the judgment of the ECJ at para 46.

[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

[30] See the Commission press release: http://europa.eu/rapid/press-release_IP-10-1462_en.htm?locale=fr.

[31] Article 99 of the Regulation.

[32] See, in particular, recital 26, article 4(5).

[33] See page 16 of Opinion 4/2007 of the Article 29 Working Party, at; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

[34] C-484/14 *McFadden v Sony Music Entertainment Germany GmbH* EU:C:2016:689.

Mr McFadden sought to rely on the intermediary defence of 'mere conduit' available under the terms of the E-commerce Directive.[35]

The European Court of Justice upheld Mr McFadden's view that his Wi-Fi provision was an Information Society Service (ISS) under EU law and therefore could avail himself of the safe harbour provisions of the E-commerce Directive. As a result, Sony could not seek damages or payment of its legal costs from Mr McFadden. The Court of Justice reiterated that EU law does not require monitoring of internet activity by ISS providers[36] but did reaffirm that Sony was entitled to seek an injunction to prevent further copyright infringements on the network and more specifically it could seek a court order forcing Mr McFadden to password protect his Wi-Fi network in the future.

The *McFadden* case attempts to balance the competing interests of consumers and copyright holders. Online copyright violations are undoubtedly a major concern, however, copyright holders appear to be moving more and more towards enforcing their rights against third party facilitators rather than the primary end-user violators. Over time, the availability of truly anonymous Wi-Fi across Europe may significantly reduce as more and more copyright holders use legal actions to force free Wi-Fi providers to only make their service available through registration and thus making identification of users much easier.

The *McFadden* case also has implications for the European Commission's Digital Market initiative, which aims to provide over 8000 additional free Wi-Fi public area spaces by 2020.[37] The project aims are laudable, however this ambitious project may be thwarted since the scheme relies on local authorities being encouraged to take on the task of delivering the networks and they may become more risk averse in light of the *McFadden* case. These local authorities may require user registration in order to gain access to the network.

However, conversely, forcing commercial free Wi-fi providers to proactively enforce and comply with data protection rules as regards IP addresses may actually provide sufficient guarantees for Wi-Fi users to continue to use such services.

Conclusion

The European Court of Justice in *Breyer* was faced with a new factual matrix as regards the legal status of IP addresses in the field of data protection. The court chose to incrementally advance the definition of personal data to include dynamic IP addresses, where circumstances exist that make it realistically possible for additional information to be combined with the IP address, thus allowing identification of the internet user.

The judgment is to be welcomed since it makes the law surrounding IP addresses more predictable, adopts a high level of privacy protection in the run-up to full-scale deployment of the new General Data Protection Regulation and helps mitigate obstacles to achieving a core objective of the EU's Digital Market agenda.

---

[35] Article 12 of the E-commerce Directive. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') *OJ L 178, 17.7.2000, p. 1–16.*

[36] Article 15 of the E-commerce Directive.

[37] The speech was delivered on the 14th of September 2016 and is available at; http://europa.eu/rapid/press-release_IP-16-3008_en.htm .