Volume 17, Issue 5
cecileparkmedia.com

# LEADING INTERNET CASE LAW

A Cecile Park Media Publication | September-October 2017

## EU Court of Human Rights rules on when monitoring work communications is lawful

Rohan Massey, of Ropes & Gray LLP, dissects the Grand Chamber's ruling that specifies the criteria to be applied when assessing whether a measure to monitor employees' communications is proportionate.

**CORRECTION** made to *Leading Internet Case Law*, Volume 17, Issue 5: In 'California Court 'SLAPPs' lawsuit against authentication service' the introduction incorrectly stated that the court found that DoubleVerify did not have grounds to file a special motion to strike. This has now been corrected to state that the court found that DoubleVerify did have grounds to file the special motion to strike. Our apologies to Karen A. Henry of Davis Wright Tremaine LLP for this mistake.




Cover image: Halfpoint / iStock / Getty Images Plus

**Editor** **Sophie Cameron** sophie.cameron@cecileparkmedia.com
**Associate Editor** **Simon Fuller** simon.fuller@cecileparkmedia.com
**Editorial Assistant** **Joel Bates** joel.bates@cecileparkmedia.com
**Subscriptions** **Conor Molloy** conor.molloy@cecileparkmedia.com
**Telephone** **+44 (0)20 7012 1387**

Leading Internet Case Law is published monthly by Cecile Park Media Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND

**Telephone** **+44 (0)20 7012 1380**
**Website** **cecileparkmedia.com**



ISSN 2399-0015

**Rohan Massey** Partner
rohan.massey@ropesgray.com
Ropes & Gray LLP, London

# European Court of Human Rights rules on when monitoring work communications is lawful

Bărbulescu v. Romania, Grand Chamber of the European Court of Human Rights, (Application no. 61496/08), 5 September 2017

The Grand Chamber of the European Court of Human Rights ('ECtHR') reversed a First Chamber decision and found that the Romanian courts, in reviewing the decision of a private company to dismiss an employee after having monitored his communications on an online messaging service, failed to strike a fair balance between the employee's right to respect for his private life and correspondence, on the one hand, and his employer's right to take measures in order to ensure the smooth running of the company, on the other. In its judgment, the Grand Chamber specifies the criteria to be applied by national authorities when assessing whether a measure to monitor employees' correspondence and other communications is proportionate to the aim pursued and whether the employee concerned is protected against "arbitrariness."

## Background

From 1 August 2004 until 6 August 2007 Bogdan Bărbulescu was employed by a private company as a sales engineer. At the company's request, he created a Yahoo Messenger account for the purpose of responding to clients' enquiries. On 13 July 2007 Mr Bărbulescu was informed by the company that his Yahoo Messenger communications had been monitored from 5 to 13 July 2007 and that the records showed he had used the internet for personal purposes. Mr Bărbulescu replied in writing that he had only used the service for professional purposes. He was presented with a transcript of his communication including transcripts of messages he had exchanged with his brother and his fiancée relating to personal matters such as his health and sex life. On 1 August 2007 the employer terminated Mr Bărbulescu's employment contract for breach of the company's internal regulations that prohibited the use of company resources for personal purposes.

## Domestic proceedings

Mr Bărbulescu challenged his dismissal in an application to the Bucharest County Court. He argued that that an employee's telephone and email communications from the workplace were covered by the notions of "private life" and "correspondence" and were therefore protected by Article 8 ECHR. He also submitted that the decision to dismiss him was unlawful and that by monitoring his communications and accessing their contents his employer had infringed criminal law. The County Court rejected the application on the grounds that the employer had complied with the dismissal proceedings provided for by the Romanian Labour Code and that Mr Bărbulescu had been duly informed of the company's regulations.

On appeal, Mr Bărbulescu repeated the arguments he had submitted before the County Court and contended in addition that that Court had not struck a fair balance between the interests at stake, unjustly prioritising the employer's interest in enjoying discretion to control its employees' time and resources. He further argued that neither the internal regulations nor the information notice had contained any indication that the employer could monitor employees' communications. Dismissing the appeal, the Court of Appeal held that the company's conduct had been reasonable and that the monitoring of Mr Bărbulescu's communications had been the only method of establishing whether there had been a disciplinary breach.

## Application to the ECtHR

Mr Bărbulescu applied to the ECtHR on the grounds that his dismissal by his employer had been based on a breach of his right to respect for his private life and correspondence and that, by not allowing his claim, the domestic courts had failed to comply with their obligation to protect his rights under Article 8. In its Chamber judgment of 12 January 2016, the ECtHR held that there had been no violation of Article 8, finding that the domestic courts had struck a fair balance between Mr Bărbulescu's right to respect for his private life and correspondence under Article 8 and the interests of his employer. The Court noted, in particular, that Mr Bărbulescu's private life and correspondence had been engaged, but considered

**The Court said that the kind of internet instant messaging service in the present case is just one of the forms of communication enabling individuals to lead a private social life. At the same time, the sending and receiving of communications is covered by the notion of 'correspondence,' even if they are sent from an employer's computer.**

continued

that the company's monitoring of his communications had been reasonable in the context of disciplinary proceedings. The case was referred, at Mr Bărbulescu's request, to the Grand Chamber.

### Applicability of Article 8

In considering the applicability of Article 8 in the current case, the Grand Chamber began by emphasising that 'private life' is a broad term not susceptible to exhaustive definition (see *Sidabras and Džiautas v. Lithuania* § 43, ECHR 2004-VIII), and that Article 8 protects the right to personal development (see *KA and AD v. Belgium* nos. 42758/98 and 45558/99, § 83, 17 February 2005), whether in terms of personality (see *Christine Goodwin v. UK*, no. 28957/95, § 90 ECHR 2002-VI) or of personal autonomy (see *Pretty v. UK,* no. 2346/02, § 61, ECHR 2002-III). The Court was also clear that the notion of 'private life' may include professional activities (see *Fernández Martínez v. Spain,* no. 56030/07, § 110, ECHR 2014). Restrictions on an individual's professional life may fall within Article 8 where they have repercussions on the manner in which he or she constructs his or her social identity by developing relationships with others.

The Court then noted that, unlike the term 'life,' the word 'correspondence' in Article 8 is not qualified by any adjective and that the ECtHR has already held that, in the context of correspondence by means of telephone calls, no such qualification is to be made. Furthermore, it has held that telephone conversations are covered by the notions of 'private life' and 'correspondence' (see *Roman Zakharov v. Russia* no. 47143/06, § 173 ECHR 2015), including where they are made from or received on business premises (see *Halford v. UK,* 25 June 1997, § 44, Reports of Judgments and Decisions 1997-III). The same, the Court said, applies to emails sent from the workplace, which enjoy similar protection under Article 8, as does information derived from the monitoring of a person's internet use (see *Copland v. UK,* no. 62617/00, § 41 ECHR 2007-I).

Applying these principles, the Court said that the kind of online instant messaging service in the present case is just one of the forms of communication enabling individuals to lead a private social life. At the same time, the sending and receiving of communications is covered by the notion of 'correspondence,' even if they are sent from an employer's computer. The Court acknowledged that Mr Bărbulescu had been informed of the ban on personal internet use laid down in his employer's internal regulations. However, it did not appear that Mr Bărbulescu was informed in advance of the extent and nature of the company's monitoring activities, or of the possibility that the company might have access to the actual contents of his communications. Further, while Mr Bărbulescu had created the Yahoo Messenger account on the company's instructions, and the company had access to it, "an employer's instructions cannot reduce private social life in the workplace to zero." In light of these considerations, the Court concluded that Mr Bărbulescu's communications in the workplace were covered by the concepts of 'private life' and 'correspondence' and, accordingly, Article 8 was applicable.

### Compliance with Article 8

The Grand Chamber recognised that contracting states must be granted a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer may regulate electronic or other communications of a non-professional nature by its employees in the workplace. Nevertheless, it said, the discretion enjoyed by states in this field could not be unlimited. The domestic authorities must ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, is accompanied by "adequate and sufficient safeguards against abuse" (see *Klass v. Germany,* 6 September 1978, § 50, Series A no. 28, and Roman Zakharov §§ 232-34). At paragraph 121 of its judgment, the Grand Chamber identified the following factors as relevant to the national authorities' assessment of whether a given measure is proportionate to the aim pursued and whether the employee is protected against arbitrariness:

- whether the employee has been notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures;
- the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy. In this regard, a distinction should be made between monitoring of the flow of communications and of their content. Whether all communications or only part of them have been monitored should also be taken into account, as should the question of whether the monitoring was limited in time and the number of people who had access to the results;
- whether the employer has provided

image: Andreas Klassen / Unsplash.com

legitimate reasons to justify monitoring the communications and accessing their actual content. Since monitoring of the content of communications is a distinctly more invasive method, it requires weightier justification;
- whether it would have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employee's communications. There should be an assessment in the light of the particular circumstances of each case of whether the aim pursued by the employer could have been achieved without directly accessing the full contents of the employee's communications;
- the consequences of the monitoring for the employee concerned and the use made by the employer of the results of the monitoring operation, in particular whether the results were used to achieve the declared aim of the measure; and
- whether the employee had been provided with adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature. Such safeguards should in particular ensure that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality.

Applying these principles, the Grand Chamber said that its task was to determine whether, in the light of all the circumstances of the case, the competent national authorities struck a fair balance between the competing interests at stake when accepting the monitoring measures to which the applicant was subjected. In this respect it acknowledged that an employer has a legitimate interest in ensuring the smooth running of the company, and that this can be done by establishing mechanisms for checking that its employees are performing their professional duties adequately and with the necessary diligence. Nonetheless, in the current case, the Court found that the Romanian courts failed to determine, in particular, whether Mr Bărbulescu had received prior notice from the company of the possibility that his communications on Yahoo Messenger might be monitored; nor did they have regard either to the fact that he had not been informed of the nature or the extent of the monitoring, or to the degree of intrusion into his private life and correspondence. In addition, they failed to determine, firstly, the specific reasons justifying the introduction of the monitoring measures; secondly, whether the company could have used measures entailing less intrusion into Mr Bărbulescu's private life and correspondence; and thirdly, whether the communications might have been accessed without his knowledge. On this basis, the Grand Chamber held, by 11 votes to six, that there had been a violation of Article 8.

## Comment

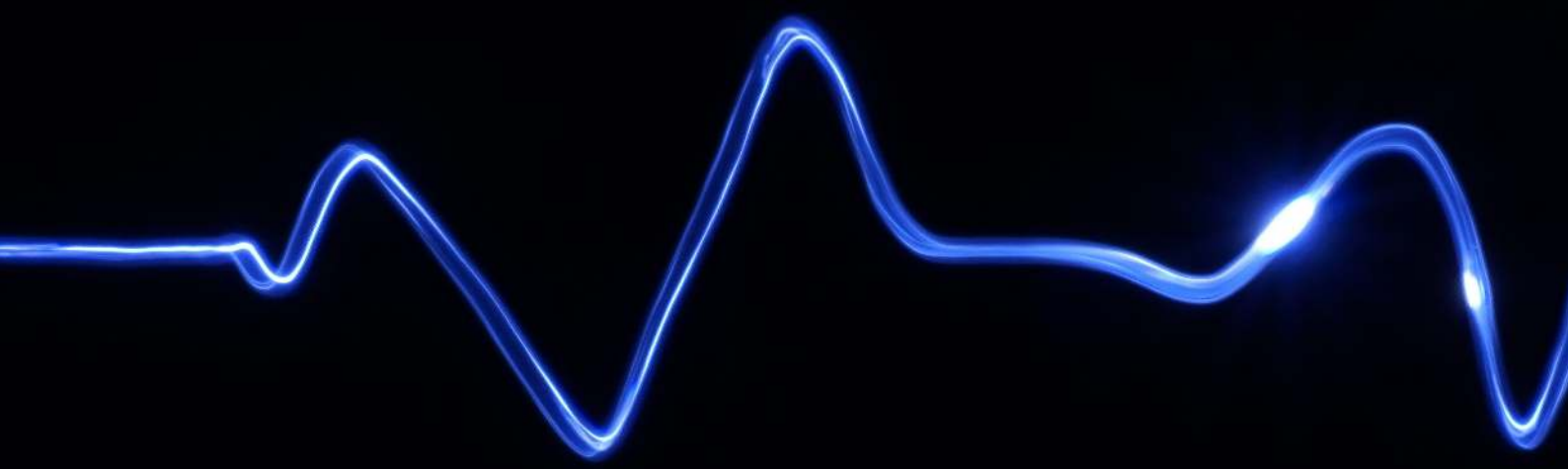
This is the first time the ECtHR, let alone the Grand Chamber, has considered the monitoring of an employee's electronic communications by a private employer. In a Q&A press release published alongside the judgment, the Court's Press Unit points out that, while the application was granted in this case, the judgment does not mean that employers can never legitimately monitor employees' communications or that they cannot dismiss employees for using the internet at work for private purposes. The thrust of the judgment is the need for national authorities, either statutory or judicial, to recognise that an employee's right to respect for his private life and correspondence cannot be expunged by the rules to which his employer subjects him and that any such rules must be proportionate and subject to adequate safeguards, including procedural safeguards, to protect the employee from their arbitrary application.

In *Copland v. UK*, the ECtHR found that the monitoring of the applicant's telephone calls, email and internet usage by the college of further education at which she was employed constituted a violation of Article 8 insofar as, at the relevant time, there was no domestic law regulating monitoring. The interference in that case was therefore not 'in accordance with the law' as required by Article 8(2). The significance of this latest case is that it establishes that it is not enough that the employer has a lawful policy in place stipulating that communications may be monitored or even that the employee has prior notice of the deployment of such measures.

The lawfulness of the employer's activities will also depend on their proportionality determined according to the further criteria identified by the Grand Chamber. Such factors will also aid the assessment of whether the employer's processing of personal data contained in an employee's workplace communications goes no further than is necessary in the legitimate interests of the employer, bearing in mind that the imbalance in the relationship between employer and employee means that consent, as a legal ground for processing, cannot always be relied on.

image: Tashdique Mehtaj Ahmed / EyeEm / Getty Images

**Abby Minns** Senior Associate
abby.minns@osborneclarke.com
Osborne Clarke LLP, London



# Technomed v. Bluecrest: UK High Court indicates broad scope of the database right

Technomed Limited and another v. Bluecrest Health Screening Limited, UK High Court, [2017] EWHC 2142 (Ch), 24 August 2017

This case saw the UK High Court indicate a broad scope for the *sui generis* database right (the 'Database Right') found within the EU Database Directive 96/9/EC, which rightsholders have found difficult to assert against a third party in light of numerous Court of Justice of the European Union ('CJEU') decisions in this area. The High Court found that a PDF of a document can be considered a database and thus the information contained can be protected by the Database Right, in a decision that may lead to more rightsholders utilising the Database Right against third parties who make unauthorised use of their databases.

In the 20 years since the Database Directive was enacted there have been relatively few cases asserting the *sui generis* Database Right against a third party. One reason for this might be that early CJEU decisions indicated it had a narrower scope than might have been anticipated - leaving rightsholders with an uphill struggle to try to assert and enforce it. However, a recent case, *Technomed Limited and another v. Bluecrest Health Screening Limited and another*, indicates that the works covered by the *sui generis* Database Right might be broader than first thought. Will this lead to an increased willingness by rightsholders to rely on the right?

## What is the Database Right?

The *sui generis* Database Right was created by the Database Directive 96/9/EC to encourage and protect the investment in databases which would not qualify for copyright protection under the national laws of many Member States. A database is defined in the Database Directive (Article 1(2)) as 'a collection of independent works, data or other materials which are arranged in a systematic or methodical way and are individually accessible by electronic or other means.'

Databases may be protected by both copyright and the Database Right. A database will be protected by copyright if 'by reason of the selection or arrangement of the contents of the database, the database constitutes the author's own intellectual creation.' This imposes a requirement of original intellectual input, in order for copyright

**Databases may be protected by both copyright and the Database Right. A database will be protected by copyright if 'by reason of the selection or arrangement of the contents of the database, the database constitutes the author's own intellectual creation.'**

to subsist. However, the Database Right protects a database where there has been qualitatively and/or quantitatively a substantial investment in either the 'obtaining, verification of presentation of the contents' of the database. Thus, pure cost and effort can be enough for the database to be protected by this right.

### The evolution of the CJEU's interpretation of the Database Right: Earlier CJEU cases indicate a narrow scope for the Database Right

Unfortunately, the economic value and impact of the new Right has been limited by the interpretations given by the CJEU.

#### *William Hill*

The *William Hill* case was a reference from the English courts concerning William Hill's use of the British Horseracing Board's ('BHB') information for the purpose of organising betting on horseracing. BHB is the governing authority for the horseracing industry in the UK. It manages a database which contains a large amount of information supplied by horse owners, trainers, horserace organisers and others involved in the racing industry. That information includes race and track details, the distance over which the race is to be run, the names of horses and jockeys entering a race, their trainers and their handicap ratings. The database costs around £4 million per year to maintain.

The CJEU held that the Database Right did not subsist in the BHB's database. It explained that for database rights to subsist there must have been "investment in the obtaining of the contents." This referred to the resources used to seek out existing independent materials and collect them in the database. Any investment in the creation of the data which made up the database was not protected. Further, the CJEU noted that the purpose of the protection by the Database Right is to promote the establishment of storage and processing systems for existing information and not the creation of materials capable of being collected subsequently in a database.

Similarly, in relation to the verification of the contents, any verification carried out in the creation of the data itself would not be covered. The CJEU noted that the expression "investment in [...] the verification [...] of the contents" of a database refers to the resources used, with a view to ensuring the reliability of the information contained in that database and to monitor the accuracy of the materials collected when the database was created and during its operation.

#### *Football Fixtures*

The CJEU was subsequently asked to decide whether football fixture lists attract Database Right protection. In three joined cases on this issue, the CJEU again referred to the fact that the Database Right did not cover the resources used for the creation of materials which made up the contents of a Database Right. The term "investment in the obtaining of the contents of a database" referred to the resources used to seek out existing independent materials and collect them in a database. Therefore, in the context of football fixture lists, "the resources deployed for the purpose of determining [...] the dates and times of and home and away teams playing in the various matches, represent [...] an investment in the creation of the fixture list." The investment described is linked to the creation of the data contained in the database and therefore is not investment of the type that can be taken into account for the purpose of determining whether the Database Right subsists. The CJEU also held that there was no investment in the verification of the database since there was no particular effort needed to monitor the accuracy of the data on league matches since the professional football leagues are so directly involved in the creation of the data.

### A change in the tide - *Football Dataco v. Sportradar*

Following the CJEU's initial decisions on the Database Right, rightsholders would have been forgiven for dismissing the Database Right as one which was narrow in scope and hard to enforce. However, the English courts gave hope to rightsholders in their decision in *Football Dataco and others v. Sportradar and others*. The database at issue was the live football data collected by Football Dataco concerning statistics in a football match such as the goals, free kicks and corners. The defendants in this case argued that this database was akin to those in *William Hill* and *Football Fixtures* since the investment made by Football Dataco was in the creation of the data. They argued that this data did not exist until it was recorded and so it was created when Football Dataco recorded it in its database. However, the Court held that the Database Right did subsist in Football Dataco's database since the data which was collected and recorded at a football match was not created by that person but merely recorded by them. As such the investment made by Football Dataco in the process of collecting the data was investment in obtaining that data. This more generous approach has now been taken a step further by the UK High Court in its latest decision.

### *Technomed v. Bluecrest* - another step towards a broader scope for the Database Right?

Technomed provides an electrocardiograph ('ECG') reporting system for doctors known as ECG Cloud. ECG Cloud enables ECG readings taken in a clinic or hospital to be analysed remotely by reporters who are not themselves carrying out the readings. ECG Cloud processes data from a mobile ECG machine through a web-based system. It is a screening service which flags up potential problems to be referred to and investigated by cardiologists. The system uses a traffic light system where green indicates a normal result, and red indicates critical or urgent abnormalities. The patient data is reviewed by a qualified cardiac physiologist who selects from a range of options from menus. The menus correspond to each ECG variable in a database. Technomed alleged infringement of its copyright and Database Right in this database (the 'Technomed Database'). The Technomed Database contains a set of classifications (the 'Classifications') such as the ventricular rate, and then contains a number of options to describe the Classifications (the 'Options') such as 'normal' or 'bradycardia' (slow), as recorded from the patient. Then, associated with each Option, is a risk status, or 'Traffic Light,' which is intended to reflect best medical practice for ECG screening purposes, and some text providing further information to the patient to help them understand the ECG reading (the 'Patient Definitions').

**It is notable also that the English courts have arguably been more willing to give a broad interpretation to the Database Right than the CJEU.**

To enable the patient to access the results of the ECG screening, ECG Cloud outputs an XML file with a standardised format. The XML file is then used to generate a report for distribution to the patient or GP. Finally, the Technomed Database also contains a feedback tool through which reviewing cardiac physiologists can edit various aspects of the reporting data. Each amendment is then reviewed and any necessary amendments are made to the components of ECG Cloud. As a result, the ECG Cloud system improves in accuracy the longer it is used.

On 31 October 2012, Technomed entered into a contract with Bluecrest to provide heart screening services. The contract was to run for over two years but, in December 2013, Bluecrest agreed to switch its services from Technomed to another company called Express. Bluecrest sent various emails to Express providing them with Technomed documents before they entered into the Express contract, asking them to replicate the service. One such document was a PDF document recording the Technomed Database. Express used this copy to create their own system.

### *Is the Technomed Database a database?*

The High Court first had to determine whether the Technomed Database fell within the definition of a database under the Database Directive. The Judge rejected the Defendants' submissions that the PDF version of the Technomed Database, whilst being a collection of independent materials, did not qualify because those materials are not separable from one another without their informative values being affected. The Judge was also not convinced by the Defendants' submission that a PDF can never be a database on the basis that it is akin to a photograph of a database rather than the database itself.

The Judge held that the Technomed Database, whether in spreadsheet or PDF format, importantly ties together a Classification, an Option and a Traffic Light. Individual Classifications are accessible either by reading the PDF with the human eye or accessing the spreadsheet electronically. By choosing one of the Options within the Classification, the relevant Traffic Light and Patient Definition are provided. The Judge went on to conclude that "the use to which the Database can be put (and indeed was put by the defendants) is no different to a telephone book (where accessing a name carries with it an address and phone number)." He therefore ruled that the Technomed Database is a database within the definition.

### *Does the Database Right subsist in the Technomed Database?*

Technomed acknowledged that, as held by the Court in the *William Hill* and the *Football Fixtures* cases, the investment cannot lie in the creation of the contents of the database. However, they argued that the Classifications, Options and Traffic Lights record objective information which they have not created. They have also taken many hours to verify the information such as through the feedback tool. They also argued that investment was made in the presentation of the data since it was arranged in a structured format. The Judge agreed that there had been substantial investment in the obtaining, verification and presentation of the contents of the Technomed Database. Therefore the Database Right was held to subsist in the Technomed Database.

### Conclusion

The Database Directive states at recital 19 that 'in addition to aiming to protect the copyright in the original selection or arrangement of the contents of a database, this Directive seeks to safeguard the position of makers of databases against misappropriation of the results of the financial and professional investment made in obtaining and collection of the contents by protecting the whole or substantial parts of a database against certain acts by a user or competitor.' Given that this legislation is now 20 years old this could be seen to be prophetic of the importance of data and databases in the digital age. However, in the light of the early CJEU decisions, to date there may have been limitations to its use. This has perhaps put off many rightsholders, and their advisers, from taking action to enforce rights in their databases.

The *Technomed* decision will be looked at with interest by rightsholders and may perhaps lead to an increase in reliance on the Database Right against third parties making unauthorised use of their databases. It is perhaps curious that the arguments over subsistence of Database Right focussed on the PDF record at all. The original database was electronic, and it would surely be arguable that it is this database which had been copied (albeit indirectly through the medium of the PDF copy). Nevertheless, the ruling that even the PDF copy was itself capable of falling within the definition opens the door to other, non-electronic databases also being protected.

It is notable also that the English courts have arguably been more willing to give a broad interpretation to the Database Right than the CJEU. The High Court (and the Court of Appeal appeared persuaded too) in *William Hill* held that the £4 million worth of investment in the BHB database was of the right nature to attract the Database Right. If the Copyright and Rights in Databases Regulations 1997 (which implemented the Database Directive) remains part of UK law post-Brexit, perhaps this could be an opportunity for the UK courts, through their interpretation of the Regulations, to broaden the scope of the Database Right further. This could prove beneficial in the digital age where the use of data is becoming increasingly valuable.

image: rawpixel.com / Unsplash.com

**Michelle Cohen** Member
michelle@ifrahlaw.com
Ifrah PLLC, Washington DC

# Second Circuit unanimously upholds Uber's mandatory arbitration provision

Meyer v. Uber Technologies Inc., United States Court of Appeals for the Second Circuit, 868 F.3d 66 (2nd Cir. 2017), 17 August 2017

The US Court of Appeals held that Uber's terms of service containing an arbitration clause was reasonably conspicuous, in a case where Uber had previously asked the Lower Court to require plaintiff Spencer Meyer to arbitrate a dispute with Uber. The case represents a victory for mobile app companies and internet businesses that seek to compel arbitration through agreements in their apps' terms of service.

In August 2017, the United States Court of Appeals for the Second Circuit unanimously ruled for Uber Technologies, Inc. ('Uber'), the ride-hailing service, holding that Uber's terms of service containing an arbitration clause was reasonably conspicuous and plaintiff Spencer Meyer assented to it by registering for an Uber account[1]. While the Appeals Court remanded the case to the Federal District Court for the resolution of related issues, the case represents a victory for mobile app companies and internet businesses that seek to compel arbitration through agreements in their apps' terms of service. Many companies view arbitration as preferable to state or federal court litigation for several reasons, including the ability to exclude class actions, confidentiality (and lack of published decisions that set precedent), reduced litigation costs, and an experienced neutral decision-maker.

## Spencer Meyer sued Uber in court; Uber seeks to arbitrate per its 'browse-wrap' terms

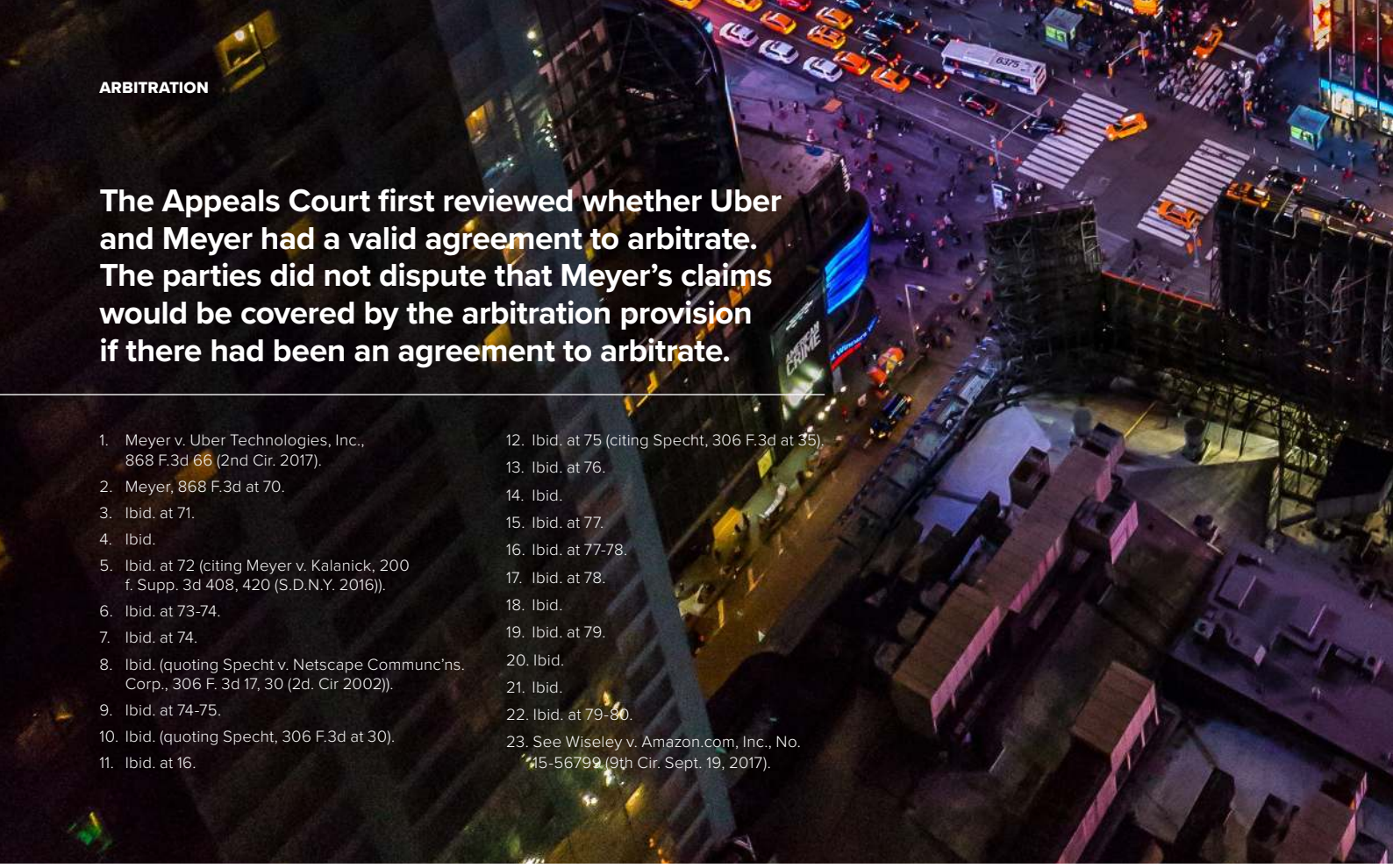
Spencer Meyer, a Connecticut resident and Uber user, sued Uber and its then CEO, Travis Kalanick, in federal District Court in New York, for illegal price fixing under Section 1 of the federal Sherman Act and a similar New York law, particularly relating to Uber's 'surge' pricing. Meyer's case was filed as a putative class action in which he sought to sue on behalf of a nationwide class who had used the Uber app to obtain a ride and paid a fare based on the Uber pricing algorithm.

In response, Uber asked the District Court to require Meyer to arbitrate his dispute with Uber. Uber based its arbitration argument on the mandatory arbitration provision set forth in Uber's terms of service, which Uber presented in the app when Meyer registered for his Uber account using the app. Meyer asserted that the terms of service were not reasonably conspicuous and that he did not agree to the arbitration provision. The Federal District Court denied Uber's motions. Absent a further ruling, Meyer could continue his potential class action in federal court. Uber appealed to the Federal Circuit Court, which ruled for Uber. The Court found that the terms of service were conspicuous. The Court also concluded that Meyer had, in essence, assented because a reasonable user would understand that he was agreeing to additional terms (and Meyer had an opportunity to click and read all those terms, including the arbitration clause).

## Uber's terms of use and arbitration provision

Uber submitted evidence documenting when Meyer registered for an Uber account and the screens and language that were presented to him. Following Meyer's entering of basic registration information and clicking 'Register,' Meyer was presented with a statement advising him that 'by creating an Uber account, you agree to the TERMS OF SERVICE & PRIVACY POLICY[2].' This capitalised phrase (appearing in blue text and underlined) contained a hyperlink that, if clicked by a user, would present Uber's Terms of Service and Privacy Policy. Meyer did not recall seeing or clicking on the hyperlink. He further declared that he did not read Uber's Terms and Conditions, including the arbitration provision[3].

Uber, like many companies, places an arbitration clause in its terms of service. The arbitration provision applicable at the



**The Appeals Court first reviewed whether Uber and Meyer had a valid agreement to arbitrate. The parties did not dispute that Meyer's claims would be covered by the arbitration provision if there had been an agreement to arbitrate.**

1. Meyer v. Uber Technologies, Inc., 868 F.3d 66 (2nd Cir. 2017).
2. Meyer, 868 F.3d at 70.
3. Ibid. at 71.
4. Ibid.
5. Ibid. at 72 (citing Meyer v. Kalanick, 200 f. Supp. 3d 408, 420 (S.D.N.Y. 2016)).
6. Ibid. at 73-74.
7. Ibid. at 74.
8. Ibid. (quoting Specht v. Netscape Communc'ns. Corp., 306 F. 3d 17, 30 (2d. Cir 2002)).
9. Ibid. at 74-75.
10. Ibid. (quoting Specht, 306 F.3d at 30).
11. Ibid. at 16.
12. Ibid. at 75 (citing Specht, 306 F.3d at 35).
13. Ibid. at 76.
14. Ibid.
15. Ibid. at 77.
16. Ibid. at 77-78.
17. Ibid. at 78.
18. Ibid.
19. Ibid. at 79.
20. Ibid.
21. Ibid.
22. Ibid. at 79-80.
23. See Wiseley v. Amazon.com, Inc., No. 15-56799 (9th Cir. Sept. 19, 2017).

time of Meyer's registration consisted of a large paragraph, titled (in bold) 'Dispute Resolution.' The provision (with certain exceptions) required the user and Uber to resolve disputes through binding arbitration. The clause further instructed, in bold, that each party waived a trial by jury and to participate in a class action[4]. In federal District Court, Uber moved to compel Meyer to arbitrate the price fixing dispute. Uber invoked the arbitration provision. The Lower Court denied the motion, finding that Meyer "did not have reasonably conspicuous notice of the Terms of Service and did not unambiguously manifest assent to the terms[5]." Therefore, according to the District Court, Meyer could not have agreed to arbitrate.

## The Second Circuit reviews whether Uber's terms of service/arbitration clause contain a valid agreement

The Appeals Court first reviewed whether Uber and Meyer had a valid agreement to arbitrate. The parties did not dispute that Meyer's claims would be covered by the arbitration provision if there had been an agreement to arbitrate. The Court noted that under the Federal Arbitration Act, Congress favours written arbitration agreements.

The U.S. Supreme Court and other courts have consistently enforced arbitration provisions[6]. However, a court must find that the parties agreed to arbitrate before a court will enforce an arbitration provision. To determine if a valid agreement exists, the court reviews applicable state contract law.

In this case, the Court applied California law (instead of New York law), though it noted that New York law on the subject is similar[7]. Under California law, 'an offeree [...] is not bound by inconspicuous contractual provisions of which he is unaware, contained in a document whose contractual nature is not obvious[8].' However, even if it is not established that the offeree had actual notice of the terms of the agreement, he or she (or it, in the case of an organisation), may be found to be on notice if 'a reasonably prudent user would be on inquiry notice of the terms[9].' The crux of the 'inquiry notice' is the 'clarity and conspicuousness of arbitration terms[10].' When a web based contract term is involved, the court looks at the 'design and content' of the interface[11]. The Appeals Court observed that it would be required to find that Meyer had "reasonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms" to conclude that a contract had been formed by Meyer with Uber[12].

Here, Uber did not require Meyer to affirmatively agree to the contract terms. Rather, at the registration button, there was a notice that the user was agreeing to the 'TERMS OF SERVICE AND PRIVACY POLICY' (with hyperlinks)[13]. The Appeals Court noted that courts in other jurisdictions have found similar agreements valid when the existence of the terms "was reasonably communicated to the user[14]."

## Was Meyer a "reasonably prudent smartphone user"?

In determining whether the arbitration provision was reasonably conspicuous, the Appeals Court stated it would consider the perspective of "a reasonably prudent smartphone user[15]." The Court further concluded that most Americans have used apps and entered into contracts via smartphone. The Court reasoned that a "reasonably prudent smartphone user knows that text that is highlighted in blue and underlined is hyperlinked to another webpage where additional information will be found[16]."

The Court examined Uber's screen design and language. It concluded that the screen was uncluttered and the reference (in caps) to Uber's Terms of Service and Privacy Policy (including the hyperlinks) appeared right below the registration buttons. Further, a user could see the entire screen "at once," without scrolling down or clicking further[17]. The Court also noted favourably that the notice of the Terms of Service was directly related and adjacent to the registration feature. The Court

image: John Baker / Unsplash.com

concluded that "a reasonably prudent smartphone user would understand that the terms were connected to the creation of a user account[18]."

Importantly, the Court found that Uber's placing of Terms and Conditions (containing the arbitration clause) only as a hyperlink did not bar a finding of reasonable notice to Meyer. Rather, Uber prompted its users to read the Terms and Conditions through the wording that '[b]y creating an Uber account, you agree[19],' and that consumers would understand that they were subjecting themselves to additional terms. The Court ultimately concluded that the hyperlinked text was reasonably conspicuous and that a "reasonably prudent smartphone user would have constructive notice of its terms" (even if many users would never read the terms)[20]. A user nevertheless would be on inquiry notice.

The Court also disagreed with the Lower Court that the arbitration clause's location within the Terms and Conditions was insufficient. Rather, according to the Appeals Court, the arbitration clause was clear, with the heading 'Dispute Resolution,' and bolded terms concerning the waiver of a jury trial and class claims[21].

### Did Meyer assent to the contractual terms (including the arbitration provision)?

The Appeals Court ruled that Meyer assented. The Court found that a "reasonable user would know that by clicking the registration button, he was agreeing to the terms and conditions accessible via the hyperlink, whether he clicked on the hyperlink or not[22]." Importantly, the Court noted that Meyer had the opportunity to review the Terms of Service prior to registering.

### Further proceedings

While the Court found the arbitration provision enforceable, it remanded the case to the District Court on Meyer's argument that Uber waived its right to arbitrate by actively participating in this litigation.

### Impact of this ruling

The Second Circuit sent a clear message that, in the smartphone age, terms and conditions available via hyperlinks (including arbitration clauses) will bind a user and be enforced by a court, provided certain conditions are met. Each case, however, will be a fact-specific review. Companies designing terms for apps and websites should carefully review how the terms are presented (including at what point in the process). The Second Circuit noted favourably that Uber's reference to its Terms and Conditions were presented in an uncluttered fashion at the point of registration. And, the hyperlinks were noticeable through the use of colour and were underlined. Further, a user saw the reference to the terms when registering, not after. The user could see the entire screen at once.

This decision may signal a trend among courts to uphold arbitration provisions in terms of use. A month later, the Ninth Circuit upheld Amazon's arbitration provision (part of its Conditions of Use), finding that an individual could not bring a purported class action asserting deceptive pricing claims against Amazon and was compelled to arbitrate[23]. In this case, Amazon presented the user with a hyperlink to its Conditions of Use on two occasions - at registration and at order confirmation. Applying Washington law, the Court found that Amazon's presentation of its hyperlinked terms was in sufficient proximity to the action buttons such that the user would have a "reasonable opportunity to understand" that by registering (and later placing an order), he/she would be bound by additional terms.

Many organisations favour arbitration clauses in consumer contracts, particularly to curb prevalent class action, to limit litigation expenses, and to keep matters confidential. Uber's victory in the Second Circuit serves as a guide for other companies, which should consider the "reasonably prudent smartphone user" when designing app Terms and Conditions and seeking to bind users.

**Marc Lempérière** Partner
marc.lemperiere@almain.fr
Almain AARPI, Paris

Image: Sami Sarkis / Photographer's Choice RF / Getty Images

# French courts rule on liability of ISPs for the cost of blocking access to pirate websites

SFR and Others v. Association of Cinema Producers and others, Court of Cassation, 6 July 2017 (C100909)

The French Court of Cassation recently approved a judgment of the Court of Appeals of Paris which analysed the balance of interest between the right of ISPs to carry out their business and the protection of intellectual property rights, finding that ISPs should be expected to bear the costs of blocking access to pirate websites.

Pirate sites have been denounced by the audiovisual industry for almost 20 years. Since they are often located in exotic jurisdictions and can easily transfer their servers from one legal entity to another, judgments obtained against such websites are very difficult to enforce. In order to assist copyright owners in mitigating the effects of these websites for the music and film industries, the European Union and national legislators decided at a very early stage to allow jurisdictions to combat these sites not where their servers or owners are physically located but where users are located, by creating authorities to sanction users of these sites (with very limited efficiency) and allowing courts to block access to these sites upon request of the copyright holders. The party liable for the costs of these technical blocking measures is not clear within EU legislation, but French courts have, in recent case law, clearly made ISPs liable for such costs. European Directive 2000/31[1] provides for a general lack of liability of internet service providers for the content they transmit, however it reserves the right for courts or administrative authorities to require service providers to terminate or prevent copyright infringement. European Directive 2001/29[2] goes further and provides that 'Member States shall ensure that rightsholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe copyright or related rights.' European Directive 2004/48 dated 29 April specifies that the measures taken 'shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.'

In France, these provisions are implemented under Article L.336-2 of the French Intellectual Property Code, which provides that when a breach of copyright occurs via an online communication service, first instance courts may order, under emergency procedures, measures that will prevent or terminate such a breach against any service providers that contribute to this breach. However, neither of the directives nor the French IP Code specify who shall bear the costs resulting from the measures imposed by such an injunction.

The Court of Justice of the European Union ('CJEU') ruled in 2011[3] that national courts are not allowed to request ISPs to actively monitor all the data uploaded by their users in order to prevent future infringement of intellectual property rights, since this would constitute a breach of the Enforcement Directive 2004/48/EC and the right of ISPs to conduct a business under Article 16 of the Charter of Fundamental Rights

of the European Union. Repeating its 2011 case law concerning trade marks[4], the CJEU also ruled that for protection measures to be fair, the measures must not be excessively costly for the ISP. In 2014[5], dealing with a new case concerning the blocking by an ISP of user access to a pirate website, the CJEU ruled that the national court did not have to specify exactly what measures were to be implemented by the ISP, provided that the ISP could prove it had taken all reasonable measures to prevent such access. Consequently, CJEU case law does not provide any guidance on how to assess whether blocking measures are too costly, but allows injunctions that do not specify the measures to be implemented, which makes the estimation of the costs of such measures impossible.

In France, the Constitutional Court[6] ruled in 2000 that the Government had to reimburse telecommunications operators for the investment they had to make in accordance with the law to allow for interception by public security, while a 2011 Decree[7] concerning the blocking of gambling sites by ISPs explicitly provides for remuneration to ISPs (to be determined by a decree which has not yet been adopted...) that are ordered to block access to illegal websites. However, on 6 July 2017, the Cour de Cassation, the French Supreme Court, approved a judgment of the Court of Appeals of Paris which analysed the balance of interest between the right of ISPs to carry out their business and the protection of intellectual property rights in a manner unfavourable to ISPs, and rejected any analogy between the two abovementioned laws and Article L. 336-2 of the French IP Code.

In 2011, a French association of film producers requested that the major French ISPs be ordered by the Tribunal de Grande Instance of Paris, under emergency proceedings, to take all measures necessary to prevent access to various streaming websites. The Tribunal[8] ordered that the ISPs take all measures necessary to prevent access to the infringing websites but ruled that the costs of such measures should not be borne by the ISPs, who were allowed to claim the costs back from the rightsholders. The producers' association appealed this decision, requesting that these costs be fully borne by the ISPs. In its judgment dated 15 March 2016, the Court of Appeals of Paris reaffirmed that claims under Article L.336-2 of the French IP Code were not civil liability claims, seeking to remedy or repair damages, but specific claims to prevent and terminate copyright infringement.

The Court of Appeals then quoted the *Telekabel* case and noted that the test to assess whether a measure was unfair, inequitable, too complicated and costly was whether this measure restrained the free use by the ISP of the resources at its disposal and stated that under the general principles of French law (without any reference to any case law embodying these principles), a party who is protecting his/her rights in law does not have to bear the costs related to the protection of those rights. The Court of Appeals then considered that on the one hand the economic equilibrium of copyrights owners was seriously threatened by the internet and they could not control the costs of infringement prevention measures. On the other hand, ISPs and web browsers provide the origin of access to the infringing sites and make a profit from this access. As a consequence, the Court of Appeals found that ISPs and web browsers should generally pay for the costs of copyright infringement prevention or termination measures, and can only obtain reimbursement of these costs by proving that a specific measure would be so disproportionate with respect to its cost or its duration that it could threaten the viability of their entire business model. The ISPs appealed this judgment in front of the Cour de Cassation but on 17 July 2017, the French Supreme Court approved the decision of the Court of Appeals of Paris, and ruled that costs of technical measures can be borne by the rightsholders only if these measures threaten the business model of the ISP.

The analysis of the Cour de Cassation may have some economic justifications, since it is indeed very difficult for copyright owners (and courts) to assess the actual cost for ISPs of implementing measures to prevent or terminate consumers' access to sites infringing copyright. However, it goes far beyond the current case law of the CJEU and makes it almost impossible for ISPs to secure payment for such measures from copyright owners. In addition, the use in the Court of Appeals' analysis of the respective financial health of ISPs and copyright owners, without any objective data, could be considered a breach of equality of the parties in front of the law, as well as a source of instability. Judges, unless the legislation expressly authorises them to do so, do not normally take into account the respective financial health of the parties in order to determine which party should bear the costs. By deciding that one party, because of its financial health, should bear the costs, the French courts have made a decision that seems more political than legal. In addition, copyright owners are not in as bad financial health as the French courts assume since they have modified their economic models to adapt to the internet (generating more revenue through live events and profiting significantly from legal streaming sites) while ISPs may in the future face new technologies (such as 5G) or an increase in competition, which could significantly alter their profitability. This judgment of the French Supreme Court seems to be founded on dubious legal considerations and goes too far in making it almost impossible for ISPs to obtain the reimbursement of their costs. On the other hand, considering the presumption that ISPs should be liable for these technical costs, demonstrating what these costs are and whether they seem proportionate to the damages caused by the offending website, would be a welcome addition to the CJEU's case law.

1. EC Directive 2000/31 dated 8 June 2000 on certain legal aspects of information society services, electronic commerce, in the Internal Market.
2. EC Directive 2001/29 dated 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in information society.
3. CJEU, Scarlet Extended SA/Société Belge des Auteurs et Compositeurs, C-70/10.
4. CJEU, L'Oréal SA v. eBay International AF, C-324/09.
5. CJEU, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, C-314/12.
6. Cons. Const, 28 Dec. 2000, n°2000-441 DC.
7. Decree n°2011-2122 dated 30 December 2011 concerning the modalities of blocking access to non-authorised online gambling or betting offers.
8. TGI Paris, 28 Nov. 2013, 2013-038010.

**In this case, the Ninth Circuit upheld the settlement approved by the U.S. District Court which provided that Google would pay a total of $8.5 million and provide information on its website disclosing how users' search terms are shared with third parties.**

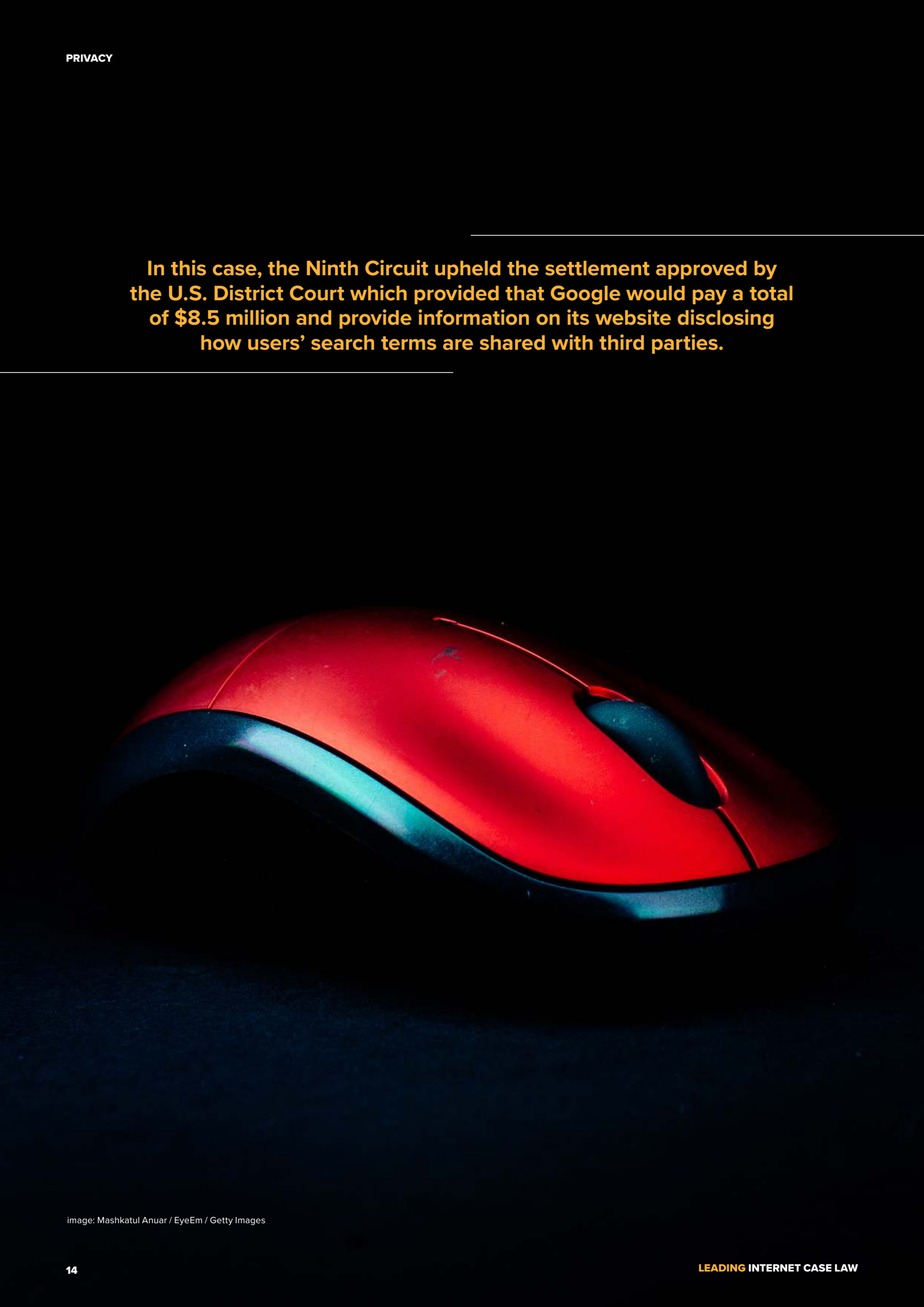


image: Mashkatul Anuar / EyeEm / Getty Images

1. Available at http://cdn.ca9.uscourts.gov/datastore/opinions/2017/08/22/15-15858.pdf

**Susan Lyon-Hintze** Partner
susan@hintzelaw.com
Hintze Law PLLC, Seattle

# In re Google Referrer Header Privacy Litigation

In re Google Referrer Header Privacy Litig., U.S. Ninth Circuit Court of Appeals (2017 BL 293516, 9th Cir., No. 5:10-cv-04809-EJD, 8/22/17), 22 August 2017

The U.S. Ninth Circuit Court of Appeals upheld a *cy pres* only award settlement, in a case in which plaintiffs alleged that Google violated their privacy by disclosing search engine data to third party websites as a consequence of 'browser architecture.'

On 22 August 2017, the U.S. Ninth Circuit Court of Appeals upheld a *cy pres* only award settlement approved by the U.S. District Court for the Northern District of California in a class action lawsuit filed against Alphabet Inc. (Google) for alleged privacy violations. (*In re Google Referrer Header Privacy Litig.,* 2017 BL 293516, 9th Cir., No. 5:10-cv-04809-EJD, 8/22/17[1]). The plaintiffs claimed that Google violated their privacy rights by disclosing search engine data to third party websites. Specifically, plaintiffs claimed violations of the Stored Communications Act (18 U.S.C. § 2701 et seq.); breach of contract; breach of the covenant of good faith and fair dealing; breach of implied contract; and unjust enrichment.

The Ninth Circuit noted the genesis of the complaint in its decision: "The claimed privacy violations are the consequence of the browser architecture. Once users submit search terms to Google Search, it returns a list of relevant websites in a new webpage, the 'search results page.' Users can then visit any website listed in the search results page by clicking on the provided link. When a user visits a website via Google Search, that website is allegedly privy to the search terms the user originally submitted to Google Search. This occurs because, for each search results page, Google Search generates a unique 'Uniform Resource Locator' ('URL') that includes the user's search terms. In turn, every major desktop and mobile web browser (including Internet Explorer, Firefox, Chrome, and Safari) by default reports the URL of the last webpage that the user viewed before clicking on the link to the current page as part of 'referrer header' information." Plaintiffs claimed in their original complaint that the referrer header could contain any search terms entered by the user, including sensitive information such as social security number, credit card number, religion, or sexual preferences which could then be revealed to third party websites receiving the referrer header.

US district courts may grant *cy pres* awards in class action settlements when there are unclaimed or 'non-distributable' portions of a class action settlement fund. In such cases the award is granted to the 'next best' class of beneficiaries for the indirect benefit of the class members. Although *cy pres* settlements are considered the exception and not the rule, such settlements are fairly common in privacy cases in the US involving large numbers of plaintiffs but with a relatively small settlement fund to distribute, typically due to inability to demonstrate enough actual harm to justify a larger award. The result is a fund that is too small to distribute among the many class members in a cost-effective manner.

In this case, the Ninth Circuit upheld the settlement approved by the U.S. District Court which provided that Google would pay a total of $8.5 million and provide information on its website disclosing how users' search terms are shared with third parties. After award of attorneys' fees and costs and awards to the three named plaintiffs who received $15,000 each, the District Court determined that the $5.3 million remaining was non-distributable to individual class members and awarded the amount to six *cy pres* institutional recipients instead.

The *cy pres* recipients were selected in part for "a record of promoting privacy protection on the Internet," and for being "capable of using the funds to educate the class about online privacy risks." The six recipients - AARP, Inc.; the Berkman Center for Internet and Society at Harvard University; Carnegie Mellon University; the Illinois Institute of Technology Chicago-Kent College of Law Center for Information, Society and Policy; the Stanford Center for Internet and Society; and the World Privacy Forum - submitted detailed proposals for how the funds would be used to promote internet privacy.

Five class members objected to the settlement, not on the basis of the amount of the settlement but on the basis that a *cy pres* only settlement was not appropriate in this case and, alternatively, objected to the choice of recipients. In its opinion upholding the District Court order approving the settlement arrangement, the Ninth Circuit pointed to the small sum each class member would have received, "The remaining settlement fund was approximately $5.3 million, but there were an estimated 129 million class members, so each class member was entitled to a paltry 4 cents in recovery - a *de minimis* amount if ever there was one."

The Ninth Circuit also rejected arguments that the *cy pres* recipients had "significant affiliations" with Google. Three of the recipients were past *cy pres* recipients of Google settlement funds and three recipients were organisations housed at class counsel's alma maters. Despite these connections, the Ninth Circuit held that the District Court did not abuse its discretion in approving the recipients, noting that "a prior relationship or connection between the two, without more, is not an absolute disqualifier" and that the District Court conducted a "careful review" of the recipient's "detailed proposals" and found a "substantial nexus" between the *cy pres* recipients and the interests of the class members.

**The BGH pointed out that there is no room for a rebuttable presumption of infringement in the case of search engines.**

**Dr Anette Gärtner** Partner
agaertner@reedsmith.com
**Iris Kruse** Associate
Reed Smith LLP, Frankfurt

image: - lexilee - / Moment / Getty Images

# Right of communication: German Federal Supreme Court applies GS Media to internet search engines

Bundesgerichtshof, Case Ref.: I ZR 11/16, 21 September 2017

While the German Federal Supreme Court ('BGH') reasoning in the *Thumbnails III* case is yet to be published, the official press release reveals that the BGH transposed the hyperlinking-related decision in *GS Media* (C-160/15) to a search engine scenario, and went a step further by highlighting that, in respect of internet search engines, there is no room for a rebuttable presumption of copyright infringement.

## *Thumbnails I*

The term 'thumbnail' is a commonly used metaphor for reproductions of pictures on a smaller scale, for example on websites or by internet search engines. For almost a decade, German courts have pondered the question of the circumstances under which such a reproduction by an internet search engine constitutes copyright infringement.

The case underlying *Thumbnails I* (GRUR 2010, 628) related to an artist who published pictures of her pieces of art on her own website. The artist did not resort to any technical means in order to prevent search engines from accessing the pictures. However, when she noticed thumbnail renditions of her art on a search engine, she brought copyright infringement proceedings.

The analysis of the BGH in *Thumbnails I* focused on national German law. Its reasoning did not mention Directive 2001/29/EC (the 'InfoSoc Directive'), which introduced the right of communication (Art. 3(1)) on a Europe-wide scale. Having said that, the BGH's line of argument did suggest that it took Recital 27 of the InfoSoc Directive and its reference to 'mere facilitators' into consideration: the judges emphasised that the defendant did not merely facilitate access to the pictures, it actively communicated the copyrighted content to users.

Nonetheless, the BGH ruled that there had been no copyright infringement. The BGH acknowledged that the artist had neither expressly, nor by implication, licensed her pictures. However, the fact that she failed to prevent access by technical means implied that she consented to the reproductions. This so-called 'simple consent' meant that the reproductions were not illegal.

### *Thumbnails II*

Just one year later, the BGH had another opportunity to express its views on the use of thumbnails on the internet. The facts underlying *Thumbnails II* (GRUR 2012, 602) were different from those underlying the previous case in that the claimant had not personally uploaded the copyrighted material (photographs) to the internet. He had, however, granted third parties licences to communicate them to the public.

The analysis provided by the BGH again focused on German national law. In the case at hand, the licences granted to customers were not limited in scope. The Court took the view that the broad licence to communicate the content to the public, by implication, also included a simple consent to reproduction by internet search engines. The claimant did not succeed in convincing the BGH that the operators of internet search engines should have also requested licences.

### Hot topic: right to communication

With the two decisions having more or less settled German case law, the discussion about thumbnails went quiet for a while. In the meantime, the right to communication under Art. 3(1) of the InfoSoc Directive became a hot topic, with the Court of Justice of the European Union ('CJEU') issuing almost 20 rulings in an attempt to delineate the scope of this right.

In *TV Catchup* (C-607/11) the CJEU stated what is seemingly self-evident when it held that a communication to the public implies two steps: first, the act of communication must take place; and second, the relevant work must be communicated to the public, i.e., to a reasonably large number of individuals.

In *Svensson* (C-466/12) the CJEU focused on this second requirement. In the underlying case, the initial communication on the internet took place with the consent of the rightsholders. Given that the alleged infringer used the same technical means of communication (i.e., the internet), the CJEU held that this subsequent communication only constituted an infringement if it was directed at a 'new public.'

The case underlying *GS Media* (C-160/15) was different in that while the content was freely available on the internet, the copyright owner had not given the green light for the initial communication to the public. Accordingly, the requirement for the communication to be directed at a new public, established in *Svensson* and subsequently confirmed in *BestWater* (C-248/13), did not apply.

However, the Court also stressed the need to balance the rights of the copyright holder on the one hand with the potential users' right to information on the other. The CJEU judges took the view that a 'filter' should be applied, according to which infringement requires that the accused either knows or ought to have known that the content was illegally placed on the internet (the so-called 'knowledge requirement'). The underlying rationale was that, if it is considered vital to have a functioning internet, it must generally be possible to use hyperlinks to published material. As an alternative, the CJEU suggested that there may be a rebuttable presumption of infringement if the communication of copyrighted material is carried out for profit.

### *GS Media* applied

The above outlines where the law stood when the *Thumbnails III* case reached the BGH. From the decision of the Court of Second Instance (Higher Regional Court of Hamburg, Beck RS 2015, 122367) and the BGH press release, we can infer that this is another case relating to copyrighted content freely available on the internet, but originally communicated without consent. The claimant allowed customers to download photographs to their computers but not to subsequently upload these photographs to the internet.

Against this background, it was inconceivable for the BGH to resort to the line of argument pursued in the previous *Thumbnails* judgments. The copyright holder clearly had not granted a simple consent to the reproduction of the photographs as thumbnails. Instead the BGH noted that the right of communication under sections 15(2) and 19a of the German Copyright Act implements art. 3(1) of the InfoSoc Directive and must therefore must be interpreted in accordance with the InfoSoc Directive. In particular, national courts are obliged to heed what the CJEU stated in *GS Media*. In *GS Media* the knowledge requirement was introduced with regard to hyperlinking to illegally published content. In *Thumbnails III* the BGH transposed this requirement to an internet search engine scenario. According to the press release, the German judges agreed with the CJEU that the internet plays a vital role in making information available to the general public. The balancing of rights therefore requires that it is generally possible to use hyperlinks. The BGH further emphasised that access to information further requires functioning search engines. On this basis, the knowledge requirement according to *GS Media* should also apply with regard to thumbnails shown by search engines. In the case at issue, the search engine operators had no reason to assume that any of the pictures had been published without prior consent.

### No room for a rebuttable presumption

Taking an even bolder step, the BGH also pointed out that there is no room for a rebuttable presumption of infringement in the case of search engines. According to the BGH, this presumption is based on the idea that someone who uses hyperlinks for profit can be expected to determine whether the content has previously been legally published. However, if the same burden were placed on the operators of search engines, they would in effect be forced to go out of business. The BGH expressly took the view that operators cannot be expected to double-check whether pictures automatically retrieved by crawlers were communicated with the rightsholders' consent.

### Conclusion

Until the full reasoning of the BGH is published, it may be somewhat premature to comment on *Thumbnails III* and its implications. The press release, however, indicates that this is a landmark decision. The BGH has contributed to the development of case law regarding the right of communication by transposing *GS Media* to internet search engines. Whether or not this should be welcomed obviously depends on one's perspective.

*Thumbnails III* appears to suggest that, if the functioning of the internet is at stake, the right of information prevails over the interests of copyright holders. The underlying question that must be answered by society, legislators and the courts is: do we think the 'search pictures' function is indispensable? If yes, then the BGH may have a point in arguing that there can be no rebuttable presumption of infringement.

**Noel Beale** Director, Competition - Regulation
noel.beale@burges-salmon.com

Burges Salmon LLP, Bristol

# Ping fined for anti-competitive online sales restrictions

UK's CMA fine to Ping, 24 August 2017

This case once again reinforces the importance to competition authorities of retailers' ability to sell products online and comes after a string of cases in recent years where suppliers have sought to restrict retailers' online activities.

The UK Competition and Markets Authority (the 'CMA') announced on 24 August 2017 that it had fined Ping Europe Limited ('Ping') £1.45 million for "banning UK retailers from selling its golf clubs online." At the time of writing we are still waiting for the full non-confidential version of the decision to be published, however, the essential specifics of the infringement are that Ping prevented two UK retailers from selling its golf clubs on their websites. Ping's intention behind the restriction appears to have been the "genuine commercial aim" of promoting in-store custom fitting of clubs (as opposed to their just being sold online). However, the CMA found that this aim could have been achieved through less restrictive means and so found that the restriction was anti-competitive.

It seems that the CMA's view was that Ping's restrictions on trading on the internet overstepped the mark in terms of what is permitted in pursuing genuine commercial aims, albeit, based on the fact that the fine imposed is relatively small, this might be interpreted as the CMA considering Ping's indiscretion to be at the less harmful end of the spectrum.

This case is the latest in a line of recent competition law cases related to restrictions imposed by manufacturers and brand owners on retailers' internet trading both in this country and across Europe. The overall message coming from those cases is that restrictions on internet trading are generally viewed unfavourably by competition authorities, as the internet is seen as such an important competitive sales channel.

## Background

Broadly speaking, agreements that prevent, restrict or distort competition are prohibited under the 'Chapter I Prohibition' (s.2 of the Competition Act 1998) where there is an effect on trade in the UK and Article 101 of the Treaty on the Functioning of the European Union where there is an effect on trade between EU Member States. However, agreements that prevent, restrict or distort competition may be exempted from the relevant prohibition(s) (Chapter I and/or Article 101) where they meet certain criteria which demonstrate that they are likely to be economically beneficial. These criteria are that the agreement in question:

- contributes to -
- improving production or distribution, or
- promoting technical or economic progress,
- while allowing consumers a fair share of the resulting benefit; and

- does not -
- impose on the undertakings concerned restrictions which are not indispensable to the attainment of those objectives; or
- afford the undertakings concerned the possibility of eliminating competition in respect of a substantial part of the products in question.

In part because these criteria are not always straightforward to apply in practice, there are also 'block exemptions' which apply to certain categories of agreement which are more specific in their terms. The key block exemption for considering restrictions in distribution agreements is the European Commission's Vertical Agreements Block Exemption (the 'VABE'). This applies both in relation to the Article 101 prohibition at EU level and the Chapter I prohibition (due to s.10 of the Competition Act 1998 which provides that exemptions at EU level are effective within the UK - so called 'parallel exemptions'). Where agreements fall outside a 'block exemption' they must be analysed individually. The VABE provides that where the marketshares of both the supplier of goods and the buyer (often the retailer in these circumstances) are below 30% agreements may benefit from the VABE provided that they do not contain certain types of restrictions (or 'blacklisted' clauses). The blacklisted restrictions in relation to online sales by retailers include:

- restrictions on the retailer's ability to set its own retail prices (albeit that it is OK for suppliers to set maximum retail prices and to communicate recommended retail prices provided these are not binding) (Article 4(a));
- restrictions on the territory into which, or the customers to whom, a buyer may sell, except the restriction of active sales into the exclusive territory or to an exclusive customer group reserved to the supplier or allocated by the supplier to another buyer (Article 4(b)(i)); and

image: Edewaa Foster / Unsplash.com

**This case is the latest in a line of recent competition law cases related to restrictions imposed by manufacturers and brand owners on retailers' internet trading both in the UK and across Europe.**

- in the context of selective distribution systems, any restriction on active or passive sales to end users (although a restriction on operation out of an unauthorised place of establishment is permitted) (Article 4(c)).

Companies found to have infringed competition law may be fined up to 10% of total group annual turnover. In addition, anti-competitive restrictions are automatically void and unenforceable, directors involved in competition law infringements (or who should have prevented them) may be disqualified and anyone who has suffered loss as a result of an infringement may bring an action for damages.

## Other recent online restrictions cases

The Ping case follows on from a number of other recent online restrictions cases across Europe, including:

- the European Court of Justice, in *Pierre Fabre* (Case C-439/09), held that restrictions on the sale of cosmetics and personal care products online were anti-competitive, as the products were not medicines and there was no need for them to be sold face to face;
- the German Bundeskartellamt's investigations into restrictions imposed by Adidas and ASICS in relation to online sales, in both cases relating to sales through online marketplaces, resulting in both companies withdrawing the relevant restrictions;
- the UK investigations into attempts by a commercial fridge supplier (ITW Limited) and a bathroom fittings supplier (Ultra Finishing Limited) to engage in resale price maintenance ('RPM') in relation to sales of their products online. In both cases, the CMA fined the companies for implementing policies that tracked retailers' online sales prices and threatened or punished retailers for selling below specified price levels; and
- in France, there is an ongoing court case between the retailer Concurrence and Samsung concerning an agreement which attempted to restrict Concurrence from retailing high-end Samsung products online.

Another relevant ongoing case in this area involves a reference to the ECJ in relation to a dispute between Coty (a leading supplier of luxury cosmetics in Germany) and Parfumerie Akzente (an authorised distributor of those products) (Case C-230/16). The dispute relates to restrictions in the agreement between the parties preventing Parfumerie Akzente from making sales on the internet through third party platforms (e.g. Amazon, eBay, etc). The difference between this case and the *Adidas* and *ASICS* cases is that Coty's defence seems to be that the restrictions are permissible because such sales may negatively impact the 'luxury image' of the products in question.

The Advocate General's view in the *Coty* case is broadly that restrictions on sales through third party platforms may be justified if the nature of the product in question requires it. Moreover, in contrast to the *Pierre Fabre* case mentioned above, the Advocate General did not regard such restrictions on third party online sales as falling outside either of Article 4(b)(i) or Article 4(c) of the VABE. However, we await the final decision of the ECJ on this.

## Conclusions

Further details are clearly to emerge about the restrictions found to be anti-competitive by the CMA in the Ping case. The arguments about whether or not the restrictions were justified may relate to whether or not Ping operated a selective distribution system in the UK and whether or not the restrictions on selling online were justified from the perspective of maintaining the image of the golf clubs concerned.

Finally, it is not clear at the date of writing whether or not Ping is intending to appeal. Given that the level of the fine is relatively low when compared to the scale of the Ping business, whether or not it does so will depend on how important it believes the relevant restrictions are to its offer to customers, and possibly whether or not it believes that the CMA is right to say that its legitimate commercial objectives could have been achieved by less restrictive means. As recognised by the EU Commission's e-commerce market investigation, the importance of the internet as a competitive marketing channel means that such issues will continue to be the focus of the activities of competition authorities across Europe for some time to come (including post-Brexit).

**Salman Waris** Partner
salman.waris@techlegis.com
TechLegis Advocates & Solicitors, India

# Supreme Court of India rules that privacy is a fundamental human right

Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India and Ors., Supreme Court of India, 24 August 2017

**The Supreme Court of India issued a landmark ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, with a nine-judge bench unanimously delivering a judgment to uphold the right to privacy as a fundamental human right under the right to life and personal liberty in Article 21, Part III of the Indian Constitution.**

## Background

The case at hand emanates from a petition challenging India's national identity scheme, Aadhaar. The judgment was made in response to a reference in which the Advocate General of India argued that the Indian Constitution does not include a fundamental right to privacy. The issue was rooted in a reference made by a three-judge bench that was hearing a challenge to the constitutional validity of the Aadhaar scheme on the grounds that it violates the fundamental right to privacy. The arguments of the Advocate General of India were based on two cases decided by the Supreme Court of India ('SC') namely: *MP Sharma v. Satish Chandra*, which was decided by an eight-judge bench in 1954, and *Kharak Singh v. State of Uttar Pradesh*, decided by six judges in 1962. The SC in both cases held that the Constitution of India does not specifically protect the right to privacy.

Initially, on 7 July 2017, a three-judge bench said that all issues arising out of Aadhaar should be decided by a larger bench and the Chief Justice of India should decide on the need for setting up a constitution bench. The matter was then mentioned before CJI Khehar who set up a five-judge constitution bench to hear the matter. However, the five-judge constitution bench decided on 18 July to set up a nine-judge bench to decide whether the right to privacy could be declared a fundamental right under the Constitution because in the 55 years that had passed since these cases were decided, there had not been a larger bench of the SC that had considered this issue, and therefore these judgments were still binding. The hearing in the case began on 19 July and concluded on 2 August. The decision to set up the nine-judge bench was taken to examine whether the two apex court judgments delivered in the cases of *Kharak Singh* and *MP Sharma*, in which it was held that privacy was not a fundamental right, were correct.

*MP Sharma* dealt with the right against self-incrimination and, while it did mention the right to privacy in passing, it was clear that these comments were stray observations at best. *Kharak Singh* was a confusing decision that held, on the one hand, that any intrusion into a person's home is a violation of liberty (relying on a US judgment on the right to privacy), but which went on to say that there was no right to privacy contained in the Indian Constitution.

## The judgment

The nine-judge bench of the SC overruled the decisions in *M.P. Sharma v. Satish Chandra, District Magistrate, Delhi* (1954), and *Kharak Singh v. State of Uttar Pradesh* (1962), which contained observations that the Indian Constitution does not specifically protect the right to privacy.

The recent judgment is a landmark ruling for an independent India. The ruling has not only learned from the past, but it also sets the wheel of liberty and freedom in motion for the future. The SC has once again emerged as the sole guardian of the Indian Constitution. Justice D.Y. Chandrachud, while delivering the main judgment, on behalf of the Chief Justice J.S. Khehar, Justice R.K. Agarwal, Justice S. Abdul Nazeer and himself, held that privacy is intrinsic to life, liberty, freedom and dignity and therefore, it is an inalienable natural right. Justices Chelameswar, Bobde, Sapre and Kaul also agreed with Justice Chandrachud's judgment. A consolidated order in the judgment holds that:

1. the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Indian Constitution; and
2. the earlier judgments of the Supreme Court in *Kharak Singh* and *MP Sharma* to the extent they held otherwise, are overruled.

The judgment runs to 547 pages in total and traces the history of constitutional jurisprudence in India with respect to fundamental rights through various SC cases, and examines scholastic articles, foreign jurisprudence, case law and international treaties.

The judgment acknowledges that:

1. privacy allows each individual the right to be left alone which is inviolable;
2. this autonomy is conditioned by the individual's relationship with the rest of society;
3. those relationships pose questions about autonomy and freedom of choice. The overarching presence of state and non-state entities regulates aspects of social existence which impact upon the freedom of the individual; and

image: John Lund / Blend Images / Getty Images

4. privacy must be analysed in an interconnected world and the SC has to be sensitive to the needs of and opportunities and dangers posed to liberty in a digital world.

The judgment states that:
"Life and personal liberty are inalienable rights. These are rights which are inseparable from a dignified human existence. The dignity of the individual, equality between human beings and the quest for liberty are the foundational pillars of the Indian constitution [...]

Life and personal liberty are not creations of the Constitution. These rights are recognised by the Constitution as inhering in each individual as an intrinsic and inseparable part of the human element which dwells within."

Tracing the evolution of privacy over the years through various cases and reports, the judgment concludes that:

"Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being."

The judgment, apart from dealing with privacy, has also dealt with a number of other aspects. The judgment authored by Justice Chandrachud rectifies the mistakes committed by the SC in the past.

Justice D.Y. Chandrachud overturned his father's (Justice Y.V. Chandrachud's) judgment in *ADM Jabalpur v. Shivakant Shukla* (1976); Justice Y.V. Chandrachud had concurred with the majority in holding that citizens' fundamental rights could be suspended during an emergency. Justice Chandrachud and the other judges in their concurring opinions upheld the dissent of Justice H.R. Khanna in *ADM Jabalpur*. Justice Khanna emphatically held that the suspension of the right to move any court regarding the enforcement of the right under Article 21, upon a proclamation of emergency, would not affect the enforcement of the basic right to life and liberty. The constitution was not the sole repository of the right to life and liberty.

The judgment also came down heavily against Justice Singhvi's judgment in *Suresh Kumar Koushal v. Naz Foundation* (2014), thereby upholding the spirit of LGBT rights.

### 'Informational privacy' and the need for data protection law

The judgment focuses on the concept of informational privacy (especially in the context of an interconnected digital world), both in the hands of state and non-state actors, including aspects of collection, use and handling of data e.g. big data, data analytics, use of wearable devices and social media networks resulting in the generation of vast amounts of user data relating to end users' lifestyle choices and preferences, the use of cookie files on browsers tracking user behaviour and for the creation of user profiles. The judgment specifically deals with informational privacy but a substantial part of the discussion relates to the handling of information by the State. The judgment contemplates a vigorous regime as per the requirements of Article 21, with the below mentioned criteria:

- existence of law to justify an encroachment on privacy;
- the requirement of a need, in terms of a legitimate state aim, that ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state action; and
- the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law.

The judgment relied upon the SC ruling in *District Registrar and Collector, Hyderabad v. Canara Bank* in relation to

continued

the informational privacy associated with the nationalised bank. The judgment also refers to in '*dicta*' the recommendations made by the 2012, Government-constituted, Expert Group Report, which proposed a framework for the protection of privacy in India. It also acknowledged the Justice B N Srikrishna committee recently set up by the Government for suggesting an appropriate data protection law in India and directs that the matter shall be dealt with appropriately by the Union Government having due regard to what has been set out in its judgment. The judgment further alludes to different facets of the data protection regime, but more as discussion points rather than binding ratio. It refers to non-discriminatory treatment on the basis of data collected. Justice Kaul also alluded to the need for a 'right to be forgotten' and suggested that EU law may serve as useful guidance on the matter.

Justice Kaul suggested that profiling of individuals by the State that leads to discrimination is not acceptable; however, such profiling can be used for the public interest and for the protection of national security. He also dealt with the right to control information in some detail and observed as follows (the observations were not distinguished as to whether they apply in relation to State and/or non-State entities):

- from the right to privacy in this modern age emanates certain other rights such as the right of individuals to exclusively commercially exploit their identity and personal information, to control the information that is available about them on the 'world wide web' and to disseminate certain personal information for limited purposes;
- there is no justification for making all truthful information available to the public. The public does not have an interest in knowing all information that is true. Which celebrity has had sexual relationships with whom might be of interest to the public but has no element of public interest and may therefore be a breach of privacy. Thus, truthful information that breaches privacy may also require protection; and
- in this regard an individual may be permitted to prevent others from using his/her image, name and other aspects of his/her personal life and identity for commercial purposes without his/her consent.

The three tests specified above that apply in relation to a fundamental right, should not necessarily apply in relation to the handling of personal data by non-state parties. If the same three tests were to be made applicable to non-State parties then the data protection regime will be very restrictive and will thwart innovation and the efficient delivery of goods and services. Therefore, the proposed data protection regime ought to make a distinction between the handling of data by State and non-State parties.

Justice Kaul further discussed the right to control and for the information to be correct on the web and alluded to the 'right to be forgotten' as essential ingredients, subject to some limitations. Further, Justice Kaul specifically dealt with privacy concerns against non-state parties, some of his key observations are below:

- a large number of people would like to keep their search history private, but it rarely remains private, and is collected, sold and analysed for purposes such as targeted advertising. Of course, 'big data' can be used to further the public interest. There may be cases where collection and processing of big data is legitimate and proportionate;
- knowledge about a person provides a power over that person. The personal data collected is capable of effecting representations, influencing decision making processes and shaping behaviour. It can be used as a tool to exercise control over people like a 'big brother' state. This can have a stultifying effect on the expression of dissent and difference of opinion, which no democracy can afford;
- there is an unprecedented need for regulation regarding the extent to which such information can be stored, processed and used by non-state parties. There is also a need for protection of such information from the State. The Indian Government was successful in compelling Blackberry to provide it with the ability to intercept data sent over Blackberry devices. While such interception may be desirable and permissible in order to ensure national security, such power cannot be unregulated.

In the past, similarly, the SC has observed the need for a law against sexual harassment in the workplace, and has directed the Government to frame such a law in the interest of protecting fundamental rights (*Vishaka v. State of Rajasthan*). One way to view the question of how the fundamental right to privacy affects non-state parties is to see the judgment as requiring that the State create a data protection law. This is to preserve citizens' informational privacy and their interest in "data protection" (per Justice Nariman) against non-state parties.

### Privacy as a right

Life and personal liberty are inalienable rights inseparable from a dignified human existence. The dignity of the individual forms the foundational pillar of the Indian Constitution along with equality between human beings and the quest for liberty. The right of privacy is a fundamental right allowing individuals to make autonomous life choices and a right which protects the inner sphere of the individual from interference from both State and non-state actors. Judicial recognition of the existence of a constitutional right to privacy is not an exercise where the Court should be seen as embarking on a constitutional function of that nature which is entrusted to Parliament nor is it in the nature of amending the Constitution.

Privacy is one of the most important rights to be protected against State and non-state actors and must be recognised as a fundamental right especially in an egalitarian society and a country which prides itself on its diversity. The privacy of the home must protect the family, marriage, procreation and sexual orientation, which are all important aspects of dignity. Let the right of privacy, an inherent right, be unequivocally a fundamental right embedded in Part III of the Constitution of India.

**Richard B. Newman** Attorney
rnewman@hinchnewman.com
Hinch Newman LLP, New York

# FTC announces first law enforcement action against individual online influencers

United States Federal Trade Commission, 7 September 2017

**The use of social media influencers has grown rapidly in an effort by brands to reach new demographics. Influencers are individuals who leverage their social media following to promote a brand or product in exchange for compensation. As influencers have gained popularity on social media platforms, the US Federal Trade Commission ('FTC') has closely scrutinised the disclosure of material connections. The FTC filed a complaint against a number of individuals who were alleged to have operated YouTube channels with the purpose of endorsing the online gambling service CSGO Lotto, without disclosing their ownership interest in the company. On 7 September 2017, the respondents settled the charges.**

As a general rule, the FTC's Testimonial and Endorsement Guides require that endorsers disclose any material connection to a brand. The FTC has previously warned numerous social media influencers against endorsing a brand or product without conspicuously disclosing material connections. A material connection can take the form of, without limitation, payment, employment, close family relationship or receipt of anything of value, including free products.

Until recently, the FTC has only initiated enforcement actions against marketers whose influencers have failed to disclose material brand connections. When acting US FTC Chair Maureen Ohlhausen took over the reins of the agency, she announced that the FTC would be returning to its core mission of traditional, bipartisan fraud enforcement, with actual consumer harm to serve as a key component in case selection. After months of intensifying regulatory scrutiny, the notice period is over. On 7 September 2017, the FTC announced three important developments pertaining to the agency's crackdown on deceptive influencer marketing.

## First law enforcement action against individual online influencers

According to the FTC, the respondents - social media influencers who operate YouTube channels focused primarily on online gaming - settled charges that they deceptively endorsed the online gambling service CSGO Lotto, while failing to disclose their ownership interest in the company.

As alleged in the complaint, the individual respondents' YouTube channels have millions of subscribers. Beginning in October or November 2015, according to the FTC, respondents operated and advertised a website, www.csgolotto.com, which offered consumers the opportunity to gamble using collectible items (or 'skins') as virtual currency. Respondents purportedly earned revenue from their CSGO Lotto skin-betting service by charging an eight percent service fee on skin betting pools.

Respondent CSGOLotto, Inc. purportedly provided the individual respondents with free skins with which to gamble on CSGO Lotto. In a video posted in early November 2015, one of the individual respondents said:

'I've been starting to bet a little bit more. ... [W]e found this new site called CSGO Lotto, so I'll link it down in the description if you guys want to check it out. But we were betting on it today and I won a pot of like $69 or something like that so it was a pretty small pot but it was like the coolest feeling ever. And I ended up like following them on Twitter and stuff and they hit me up. And they're like talking to me about potentially doing like a skins sponsorship like they'll give me skins to be able to bet on the site and stuff. And I've been like considering doing it.'

Between mid-November 2015 and June 2016, individual respondents allegedly posted videos to their respective YouTube channels showing themselves gambling on CSGO Lotto. According to the FTC, these videos promoted CSGO Lotto and encouraged viewers to use the gambling service.

Between mid-November 2015 and June 2016, the first individual respondent allegedly posted at least 13 promotional videos to his YouTube channel showing himself gambling on CSGO Lotto, including ones with titles such as, 'HOW TO WIN $13,000 IN 5 MINUTES (CS-GO Betting),' '$24,000 COIN FLIP (HUGE CSGO BETTING!) + Giveaway,' 'HUGE WINS (And Losses) - CounterStrike Betting Challenge #2 (CSGO Skins),' and 'CS-GO Betting - Part 3 - HUGE $1000+ COIN FLIP BET! (Duel Arena Skin Gambling).' As set forth in the complaint, nowhere in his videos promoting CSGO

**As described by the FTC, consumers who saw promotions of CSGO Lotto by the individual respondents were unlikely to learn of the connection between the individuals and CSGO Lotto.**

continued

Lotto or in the videos' descriptions did the first individual respondent disclose that he was an officer and owner of the company operating CSGO Lotto or that he was gambling with free skins provided by that company. In the promotional videos showing him gambling on CSGO Lotto, the FTC also took issue with the individual respondent not mentioning any connection between himself and CGSO Lotto.

Of additional concern to the FTC, the first individual respondent allegedly disseminated tweets that promoted CSGO Lotto and linked to his promotional videos. One such tweet read, 'Made $13k in about 5 minutes on CSGO betting. Absolutely insane. Reactions here : [YouTube link].' (6 March 2016 tweet by @TmarTn). An Instagram post by that same respondent allegedly showed screenshots of him winning two betting pools on CSGO Lotto with the caption, 'Unreal!! Won two back to back CSGOLotto games today on stream - $13,000 in total winnings.' According to the FTC, nowhere in his social media posts promoting CSGO Lotto did he disclose any connection between himself and CGSO Lotto.

Between January and June 2016, the second individual respondents allegedly posted at least seven promotional videos showing himself gambling on CSGO Lotto, including ones with titles such as, 'INSANE KNIFE BETS! (CS:GO Betting),' 'CRAZY 6 KNIFE WIN!!! (CS:GO Betting),' and 'ALL OR NOTHING! (CS:GO Betting).' According to the FTC, this individual's videos promoting CSGO Lotto garnered more than 5.7 million views.

However, the FTC complained that nowhere in his videos promoting CSGO Lotto or in the videos' descriptions did the individual respondent disclose that he was an officer and owner of the company operating CSGO Lotto. According to the FTC, in at least five of his videos promoting CSGO Lotto, the individual respondent did not mention any connection between himself and CSGO Lotto. While each of these videos' description boxes included the statement 'This video is sponsored by CSGO Lotto!," the disclosure appeared in the description boxes "below the fold" where it would not be visible without consumers having to click on a link and perhaps scroll down. Compounding the situation, according to the FTC, the second individual respondent disseminated tweets that promoted CSGO Lotto and did not disclose any connection between himself and CGSO Lotto. These tweets allegedly contained statements such as:

'CRAZY 6 KNIFE WIN!!! (CS:GO BETTING): [YouTube link] ... OUR LUCK HAS CHANGED!!! 2016 IS THE YEAR OF THE KNIFZ! Site Used ? CSGO LOTTO: https://csgolotto.com Big thanks to Flux Pavilion for letting me use his music ...'

'Bruh.. i've won like $8,000 worth of CS:GO Skins today on @CSGOLotto I cannot even believe it!'

'I lied... I didn't turn $200 into $4,000 on @CSGOLotto...I turned it into $6,000!!!! csgolotto.com/duel-arena.'

As described by the FTC, consumers who saw promotions of CSGO Lotto by the individual respondents were unlikely to learn of the connection between the individuals and CSGO Lotto. Even those who did learn of a sponsorship relationship with CSGO Lotto would not have learned that they were officers and owners of the company operating CSGO Lotto, and thus had a vested interest in the success of the service, or that they were gambling with skins that were provided by that company.

The individual respondents also allegedly used an 'Influencer Program' to encourage certain online influencers "to post in their social media circles about their experiences in using" CSGO Lotto. The FTC specifically cited that respondents contractually prohibited the influencers from making "statements, claims or representations [...] that would impair the name, reputation and goodwill of" CSGO Lotto, in the complaint. Payments to influencers were in US dollars, skins credits, or a combination of both and ranged from $2,500 to $55,000.

The influencers the individual respondents hired promoted CSGO Lotto on YouTube, Twitch, Twitter, and Facebook. According to the FTC, numerous resulting YouTube videos of influencers gambling on CSGO Lotto did not include any sponsorship disclosure in the videos themselves and if they included sponsorship disclosures in the description boxes below the videos, they only did so "below the fold." Numerous resulting social media posts by influencers promoting CSGO Lotto allegedly did not include any sponsorship disclosures. The FTC alleged that the acts and practices of the respondents constituted unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

The FTC asserted that the videos of the individual respondents gambling on, and their social media posts about, CSGO Lotto represented, directly or indirectly, expressly or by implication, a reflection of independent opinions or experiences of impartial users of the service. However, in truth and in fact, the videos of the individual respondents, and other influencers gambling on CSGO Lotto and the social media posts about CSGO Lotto, did not reflect the independent opinions or experiences of impartial users of the service. Given the individual respondents' ownership interest in the company operating CSGO Lotto, as well as the other influencers that were paid to promote CSGO Lotto and that were prohibited from impairing its reputation, the FTC asserted that the respondents' representations were false, misleading and deceptive, in part, because these facts would be material to consumers in their decisions regarding using CSGO Lotto.

The FTC order settling the charges requires respondents to clearly and conspicuously disclose any material connections with an endorser or between an endorser and any promoted product or service. "Consumers need to know when social media influencers are being paid or have any other material connection to the brands endorsed in their posts," said Ohlhausen. "This action, the FTC's first against individual influencers, should send a message that such connections must be clearly disclosed so consumers can make informed purchasing decisions."

## New warning letters

In April 2017, the FTC sent more than 90 educational letters to social media influencers and brands. The FTC recently announced that it has sent 21 follow-up warning letters. The first round of educational letters informed influencers that if they are endorsing a brand and have a 'material connection' to the marketer, this must be clearly and conspicuously disclosed, unless the connection is already clear from the context of the endorsement. The most recent warning letters cite specific social media posts of concern to FTC staff and provide details on why they may not be in compliance with the FTC Act as explained in the Commission's Endorsement Guides.

For example, some of the letters point out that tagging a brand in an Instagram picture is an endorsement of the brand and requires an appropriate disclosure. The letters ask that the recipients advise FTC staff as to whether they have material connections to the brands in the identified posts, and if so, what actions they will be taking to ensure that all of their social media posts endorsing brands and businesses with which they have material connections clearly and conspicuously disclose their relationships. The FTC is not disclosing the names of the 21 influencers who received the warning letters.

## Updated guidance

In another interesting development, the FTC has recently announced updates to staff guidance for social media influencers and endorsers. The FTC's Endorsement Guides: What People are Asking ('Guides'), is a staff guidance document that answers frequently asked questions. The Guides were previously revised in 2015. The newly updated version includes more than 20 additional questions and answers addressing specific questions social media influencers and marketers may have about whether and how to disclose material connections in their posts. The new information covers a range of topics. Highlights include:

- Free products, travel or other incentives for reviews: The updated FAQs emphasise the importance of properly disclosing any material connection, including free or discounted products, travel or accommodation, provided by an advertiser to a reviewer. Even reviews made in exchange for charitable donations should be disclosed. The disclosure requirements apply even where the incentive is not contingent on the recipient posting a review. Interestingly, the FAQs advise that if free products are given to some reviewers, advertisers should disclose next to any average or other summary rating that it includes reviewers who were given free products.
- Details of compensation: Although endorsers must disclose the fact that they were compensated for a review (e.g., by using a 'paid' hashtag), they are not required to detail the amount of the compensation received. The FTC's position is that negligible compensation that would not affect the weight average readers would give the review may not need to be disclosed at all.
- Tagging brands: The FAQs explicitly state that tagging a brand in a post is an endorsement of the brand and could require a disclosure if the endorser has a relationship with that brand. For example, if someone posts a picture of herself and tags the brand of the dress she is wearing, if she was given the dress by the brand, she must disclose the relationship.
- Instagram, Snapchat and other social media platform disclosures: The updated FAQs address questions relating to specific social media platforms including Instagram and Snapchat. Generally speaking, social media or blog disclosures must be clear, conspicuous and prominent. They should find the reader and be difficult to miss. Consistent with the Agency's recommendations in warning letters to social media influencers, the FAQs reiterate that endorsement disclosures in Instagram posts should be present in the picture or within the first three lines of the description. A reader should not have to click 'more' in order to see the disclosure. Disclosures should be superimposed over the video or image in a manner that is noticeable and plainly discernable for Instagram and Snapchat Stories.
- Wording of social media disclosures: Using '#ad' or '#sponsored' may constitute a sufficient disclosure of sponsored content, provided that it is clear, conspicuous and prominent. Saying 'thank you,' without further clarification, is most likely insufficient. The FTC specifically advises against use of '#ambassador' in a tweet. Unless it is coupled with the full name of the sponsoring brand, it is ambiguous (e.g., '#[BRAND] Ambassador'). Similarly, '#employee,' without more, may not adequately disclose the material connection between the endorser and the brand.
- Do not assume that built-in features on social media platforms that allow users to disclose paid endorsements are sufficient if the material connection is not clearly and conspicuously disclosed.
- A disclosure on one social media platform does not relieve an endorser of the obligation to also make the relevant disclosure on other social media platforms where sponsored content is posted.

Placement and context considerations are critical. Disclosures must be transparent, unambiguous, conspicuous and prominent. Influencers are advised to keep in mind that the UK and other countries have similar laws and policies with respect to paid endorsements, and take steps to ensure compliance.

## Takeaway

The FTC is closely monitoring marketers, their agencies and their influencer networks. Influencers themselves are now fair game. Social media influencers must "clearly and conspicuously" disclose when they have a material connection with a brand. It is dangerous to assume that followers know about brand relationships. Ensure that sponsorship disclosures are difficult to miss. Never assume disclosures built into social media platforms are sufficient. Sponsored tags, including tags in pictures, should be treated like any other endorsement. Do not use ambiguous disclosures like 'Thanks,' '#collab,' '#sp,' '#spon' or '#ambassador.' On image-only platforms like Snapchat, superimpose disclosures over the images. The FTC has warned against relying upon disclosures that people will see only if they click 'more.'


image: William Iven / Unsplash.com

**José Lema** Lawyer
jlema@ecija.com
Ecija, Madrid

# Spanish Data Protection Authority fines Facebook €1.2 million for data protection infringements

The Spanish Data Protection Authority, following an investigation, has found that Facebook processes data, including sensitive data, for advertising purposes without obtaining adequate consent; it also found that Facebook does not delete users' data when requested to do so or where the data becomes no longer relevant. The Spanish Data Protection Authority's findings, and subsequent fine handed down to Facebook, represent the consequences of broader changes to how data processors are viewed within the EU.

## Background

European data protection authorities have had Facebook in their sights for quite some time and not without reason: the American giant has been less than transparent in communicating how personal data is processed on its platform. However, only recently has the context shifted to one where the general public is much more conscious of data protection related issues, which has allowed the Spanish Data Protection Authority (hereinafter, 'AEPD') to confidently carry out an investigation in the context of a sanctioning procedure.

The AEPD took it upon itself to investigate Facebook's processing of personal data and whether it was compliant with the European regulations and the Spanish Data Protection Law (hereinafter, 'LOPD'). On the date the resolution was issued, the AEPD was able to use arguments backed by the CJEU and the Spanish Supreme Court to pin down Facebook Inc. to the local jurisdiction and apply the LOPD in full force. The investigation went on to find that Facebook Inc. was breaching several obligations of the LOPD, namely duly informing users about the data processing, duly obtaining users' consent for this processing, and duly removing data after being requested to do so or when data is no longer relevant.

## Details of the proceeding

### *Facebook, Inc. as data controller*

The AEPD did not accept Facebook's argument that the company that is bound by European data protection regulation is actually Facebook Ireland, Ltd, as accepted by European users when registering with the social network. The AEPD's counter argument was that, based on the Spanish Supreme Court's case law (STS 1384/2016), Facebook Inc. would be considered a data controller in any case:

"In its Opinion 1/2010, the Article 29 Working Party stated that 'The concept of controller is autonomous [...], and functional, [...] and thus based on a factual rather than a formal analysis.' [...] Google Inc., which manages the search engine Google Search, is a personal data controller, since it determines the ends, the conditions and the methods for the personal data processing."

Facebook Inc. is therefore identified as a data controller for users in the European Union, given its key role in the data processing.

### *Application of the LOPD*

Following on from this premise, the AEPD analysed whether the LOPD is applicable to Facebook Inc., which would be the case for a data controller not established in Spain if a) the processing is carried out in the context of the activities of an establishment of the data controller, where the establishment is located in Spain, and b) where means located in Spain are being used in the processing of personal data. The AEPD quoted the CJEU judgment of 13 May 2014, reiterating that:

"[...] it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable."

Based on that reasoning, the AEPD found that Facebook Spain, S.L. could be considered an establishment located in Spain. The AEPD argued that the main purpose of Facebook Spain, S.L. is to attract advertisers to the platform, an activity that is causally linked with the data processing of Facebook Inc. This would guarantee the application of the LOPD to the facts at hand.

Furthermore, the AEPD also stated as a secondary argument that Facebook Inc. is using means located in Spain for the processing of personal data, namely the user's computers and the cookies therein installed. This alone would also be enough grounds for the LOPD to be applicable to the case at hand.

*Information duty*

The AEPD found that Facebook had infringed its duty to duly inform users regarding the collection and processing of data, the methods of processing and its purpose. The AEPD reached this conclusion after finding that:

- Facebook misguides users when obtaining consent, not disclosing that personal data other than that directly provided by the user will also be collected and processed. The use of multi-layered information makes it difficult for the user to grasp all relevant information.
- A 'data policy' is linked at the moment of registry, without making explicit reference to data protection. Accessing this policy is not mandatory prior to registration.
- Users are not provided with a list of the data that will be collected and processed.
- No options for guaranteeing parental consent for minors are enabled. Furthermore, advertising campaigns can target minors.
- Users are not warned that the cookies installed in their browsers can gather information even when they are not logged into the network.

*Duty of obtaining consent*

The AEPD found in its investigation that Facebook had infringed its duty to obtain free, unequivocal, specific and informed consent from its users. The AEPD reached this conclusion after finding that:

- The consent cannot be specific where the information is given by means of imprecise wording which does not allow users to understand how the data is processed and the purpose of the processing.
- The data collected is not proportional in connection with the purpose of the processing, much less where the user is giving misinformed consent.
- The word 'finished,' instead of 'I accept,' is used when completing user registration. Furthermore, users are not required to have consulted the data privacy policy prior to consenting.
- Considering that the information shown by Facebook can confuse the average user of new technologies, the consent can never be unequivocal or specific.

*Sensitive personal data*

Some duties are stricter when referring to the sensitive personal data of Facebook users:

- Facebook collects and processes sensitive personal data, which it uses to build profiles, even after informing the user that his/her sensitive personal data will not be used for advertising.
- The tools provided to advertisers allow them to target the public based on sensitive data such as sexual life, beliefs or health.
- For sensitive data, the consent must be explicit and in writing, and Facebook does not comply with these requirements.

*The duty to remove data*

The AEPD found that Facebook had infringed its duty to remove personal data where it is no longer necessary for the purpose for which it was collected. The AEPD reached this conclusion after finding that:

- Where a user configures their privacy settings so that ads are not served based on personal data, the profiling data collected by Facebook is not erased but stored.
- The IP addresses from where connections have been established are stored for at least 11 months, which could lead to the identification of the physical location of a user.
- After deletion of an account, a cookie associated with the cancelled profile could be associated to a new user registered with the same email for up to 17 months.

**Sanctions**

The AEPD imposed the following fines:

- For breaching Article 6.1 of the LOPD, constituting a serious infringement: €300,000.
- For breaching Article 7 of the LOPD, constituting a very serious infringement: €600,000.
- For breaching Article 4.5 of the LOPD, constituting a serious infringement: €300,000.

The AEPD handed down the largest sanction available for each of the infringements, taking into account aggravating facts such as the infringement being continued, the volume of the processing carried out, the link between Facebook's activity and the personal data processing, Facebook's turnover created as a direct result of the infringements and Facebook's intentionality in its conduct.

**What the decision tells us about large-scale data processing**

The decision itself does not mark a sudden change of direction in the manner in which data processors are regarded in Europe. Rather, the AEPD resolution is but a consequence of a much broader and slower process, of which the ultimate result is the EU General Data Protection Regulation (the 'GDPR').

This Regulation is what should be taken into account by large scale data processors in their handling of personal data. Data controllers that process personal data of European individuals have been sufficiently warned and given enough time to accommodate the requirements of the GDPR. This fine is but a reminder that local data protection agencies will start taking measures if they believe that the provisions of the GDPR or the local regulations are not being complied with.

Arguments for pinning down international operators to not only the European, but also local jurisdiction, are now fully backed by the CJEU and even local Supreme Courts. This current doctrine is much more in line with what the GDPR has in store: Article 2 states that the GDPR shall apply to controllers not established in the EU where the processing of personal data of European data subjects is related to (a) the offering of goods or services; or (b) the monitoring of their behaviour.

It is clear that the activity of many international operators, including Facebook, falls within those definitions, and therefore they will have to comply with the dispositions of the European Regulation when it enters into force. Finally, this decision corroborates that businesses, European and non-European, will have a harder time complying with European data protection regulations, which will result in a double-edged effect.

On the one hand, non-EU companies will be more dubious about offering their services in Europe, where those services imply the processing of personal data - which might be especially harmful, considering the universality of internet-borne, information technology services. On the other hand, European companies, especially newly formed companies, will have to bear a heavy compliance burden that simply will not exist for non-EU competitors.

All of this could result in innovation stagnation for European companies, which may become incapable of competing in an environment based on novelty and speed.

# LEADING INTERNET CASE LAW

**More publications** from Cecile Park Media


## Save up to 30% with print and digital edition bundles

**Buy 2 Cecile Park Media titles and save 10%**

**Buy 4 Cecile Park Media titles and save 15%**

**Buy 6 Cecile Park Media titles and save 20%**

**Buy all 8 Cecile Park Media titles and save 30%**

For subscriptions call us now on +44 (0)20 7012 1387
or visit cecileparkmedia.com

Each of the publications are individually priced, so please contact us for specific information on pricing. We offer four subscription types: single-user, site licence, academic and corporate, all of which can be tailored to your specific needs and come with hard-copy and online access.

Leading Internet Case Law is published monthly by Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND

Telephone +44 (0)20 7012 1380 Website cecileparkmedia.com