Privacy, Expression and the World Wide Web. Shall we Forget?

Dr. Katy Ferris[1]

ABSTRACT

Google v Spain[2] is an important judgment of the Court of Justice of the European Union which has important implications for the rights of individuals' privacy, the Court's use of a purposive method of interpretation, the regulation of search engines based outside of the EU, the interaction between the Treaty on the Functioning of the European Union, the Charter of Fundamental Rights of the European Union and European Convention on Human Rights, and international laws. The case establishes that operators of search engines located outside of the EU may be subject to the EU data protection laws (Directive 95/46/EC) and individuals, in certain circumstances, have the right to request that links to personal data held on-line be removed.

1. BACKGROUND

The European Union (EU) Directive 95/46/EC – the Data Protection Directive[3] (DPD) - was adopted in 1995, when the World Wide Web was still in its infancy, and most Web-recognisable brand names did not exist. The first version of the code establishing the Google search engines was written in 1996, and the company was officially founded in September 1998 – shortly before the deadline for transposition of the Directive.

Directive 95/46/EC provides:

> (2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;
>
> (10)… the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms… and in the general principles of Community law;.. for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.

The centrepiece of EU legislation on personal data protection (the DPD) was adopted with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. The DPD adopts a 'holistic' approach to data protection applying minimum principles to all stages of data processing, whilst generally not distinguishing between collection, storage, use or disclosure. [4] The relationship was examined between the DPD, the Charter of Fundamental

Rights of the European Union and the existence of search engines.

The DPD thereby creates a system of controlling the ways in which data processing is handled within the EU and provides the data subject with a mechanism to correct inaccurate data and/or object to the data concerning him/her. The case subject to this article required an interpretation of the Directive's provisions in light of the fundamental rights and freedoms laid down by the Charter.[5]

Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), establishes the principle that everyone has the right to the protection of personal data concerning him or her. Moreover, Article 16(2) TFEU, introduced a specific legal basis for the adoption of rules on the protection of personal data. Article 8 of the Charter of Fundamental Rights of the EU enshrines protection of personal data as a fundamental right. Yet, pending the completion of negotiations for a revision of the Directive proposed by the EU Commission in 2012,[6] this legislation has remained applicable to the World Wide Web as it has developed since 1995.

1.1. PERSONAL DATA AND RESPONSIBILITY

Google v Spain is the first case where the Court of Justice of the European Union (CJEU) has been required to interpret the DPD in relation to internet search engines.[7] Many years of controversy as to whether (and if so, how) the DPD applies to key elements of the Web, such as social networks, search engines and cookies have culminated in this judgment. The first case of significance in relation to *Google v Spain* was heard in 2003. In the *Lindqvist* case[8] the CJEU held a person who publishes personal data on a website processes the data and the publisher of the website is the data controller i.e. the person who has primary responsibility for data protection compliance.

Mrs Lindqvist was an active member of her church in a parish in Sweden. As part of a computer course, Lindqvist had to set up an internet home page, she did so by creating a site giving information to church parishioners. Mrs Lindqvist included information about herself and eighteen fellow church volunteers. This information included some full names, telephone numbers and references to hobbies and jobs held by her volunteer colleagues. In relation to one colleague, Lindqvist also revealed that she had injured her foot and was, on medical grounds, working part-time.

Lindqvist did not obtain her fellow volunteers' permission to post information about them on her website. In fact, Lindqvist failed to inform them about the postings before publication, although she did remove the web pages as soon as she received a request from her colleague to do so.

Mrs Lindqvist was fined SEK 4,000 (approximately £300) for (a) processing personal data by automatic means without properly notifying the Datainspektion (the Swedish supervisory authority for the protection of electronically transmitted data); (b) transferring individuals' personal data, without consent, to countries not having similar levels of personal data

protection; and (c) processing individuals' sensitive personal data (the information concerning the volunteer with the foot injury) without consent.

Lindqvist appealed. She contended that posting information on an Internet website did not amount to 'processing personal data' within the meaning of the DPD and that posting information on a website did not amount to a transfer of data to a third country. She also contended that the DPD does not apply to non-profit activities and that the sanctions she faced for violating the data protection requirements infringed her freedom of expression.

The CJEU determined that posting individuals' names and telephone numbers (as well as information regarding their working conditions and hobbies) on a website did constitute the 'processing' of personal data for the purposes of the DPD. Having made this initial determination, it moved on to consider whether posting personal data on a website could be construed as 'transferring' such data to a third country. On this point, the CJEU supported the arguments made by Lindqvist, concluding that website operators posting personal data on-line are not subject to the legal regime governing the transfer of personal data unless (i) they actually send the personal information to Internet users who did not intentionally seek access to the webpages, or (ii) the server infrastructure is located in a non-EU country. This was a somewhat surprising decision at the time as it was inconsistent with the understanding held by many legal and Internet commentators and the interpretation of the law by national data protection authorities. It did offer some guidance on what would be considered as a 'transfer' within the context of an Internet post.

Several issues, however, remained unanswered following the case which makes *Google v Spain* so significant. *Lindqvist*, unlike *Google v Spain* did not involve a profit making company collecting large amounts of data about individuals. The data controller in *Lindqvist* had the intention to enhance the community in which she lived in and through connection with others. There was no embarrassment on the part of the individuals and when she was asked to take down the material, she did. The CJEU did not address Lindqvist's claims that the restrictions imposed by the DPD limited her freedom of expression. It was arguably a minor exposure of limited personal information. Lindqvist's lawyer at the time stated that 'This decision emphasises the wide-reaching and indiscriminate nature of the European Union's Data Protection Laws.'[9] Finally, unlike *Lindqvist*, *Google v Spain* concerned the use of search engines. These issues were addressed in *Google v Spain*, perhaps with unfortunate consequences.

2. THE ISSUE IN *GOOGLE V SPAIN*

In early 1998, a newspaper (*La Vanguardia*) published, in its printed edition, a notice of a real estate auction in respect of the property of Spanish citizen Mario Costeja González for unpaid debts. He subsequently paid the debts and the auction of the house did not take place. Later, the publisher made the article available electronically. Ten years on, Google searches of the name Mario González brought up the newspaper advertisement. In November 2009, no longer wishing to have this record of an old newspaper report on his

financial history (concerning social security debts) to be available,[10] González contacted the publisher (La Vanguardia Ediciones SL) arguing the information was no longer of relevance and should be removed. The publisher responded that erasure of the data was not appropriate due to it being effected by the (domestic body) Ministry of Labour and Social Affairs. In February 2010, González contacted Google Spain SL requesting that search results not provide links to the newspaper article when his name was entered into its search engine. This request was forwarded to Google Inc. in the USA, as Google Spain SL considered it was the relevant organisation providing the Web-search service.

Following these actions, González complained to the Spanish data protection authority (AEPD)[11] that the publisher should be required to remove or rectify the information so his personal data was protected, and that Google Spain SL / Google Inc. be required to remove or conceal his data regarding links to the newspaper article when his name was entered into the search engine. On 30 July 2010, the AEPD rejected Costeja's complaint against the publisher of *La Vanguardia* on the grounds that 'the publication of the information was legal and was protected by the right to information.'[12] The information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible.

However, with inconsistency, it upheld his complaint against Google Spain and Google Inc., ordering the search engine to eliminate approximately 100 links from all future searches for Costeja's name. The AEPD considered in this regard that operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society. The AEPD took the view that it has the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considers that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense, and this would also encompass the mere wish of the person concerned that such data not be known to third parties. The AEPD considered that that obligation may be owed directly by operators of search engines, without it being necessary to erase the data or information from the website where they appear, including when retention of the information on that site is justified by a statutory provision.[13]

Google Spain SL and Google Inc. appealed to the Audiencia Nacional (National High Court) which, on a preliminary reference, referred questions on the meaning of the DPD to the CJEU.

3. THE CJEU's RULING

The CJEU addressed four key issues in its judgment:

3.1. THE MATERIAL SCOPE OF THE DIRECTIVE, I.E. WHETHER IT APPLIES TO SEARCH ENGINES

Until *Google v Spain*, It was widely assumed that further processing of the personal data by services such as search engines fell outside the scope of data protection law as the publisher of a website could restrict search engine indexing through the configuration of its website. This approach was the one advised to the CJEU by the Advocate-General (A-G) to be taken when dealing with this issue. The CJEU somewhat surprisingly disagreed with the A-G's view that Google was not a data controller when it indexed personal data for its search engine.

A-G Jääskinen had argued the position in *Lindqvist* that the publisher of a webpage containing personal data is a data controller. However, he was of the view that a person is not a data controller unless he or she is aware of the existence of a defined category of personal data. In light of his view as to how a data controller should be defined, A-G Jääskinen felt that because Google does not have an awareness of personal data other than as a statistical fact, and since the personal data is assembled randomly with all the other internet data, Google indexes including non-personal data should not have been considered to establish Google as a data controller. The A-G was of the view that search engines providing, as they do, an important service for internet users, should arguably enjoy a degree of exemption from data protection liability analogous to that which applies to e-commerce intermediaries providing information society services on an automated, passive, technical basis with no control over the information carried on the service.

In the event that the CJEU did not agree with his submission that Google is not a data controller, the A-G considered questions relating to a right to be forgotten. He held that the rights of freedom of information and expression took precedence over any such right to erasure, and urged the Court not to allow case-by-case resolution of such conflicts as that would likely lead to the 'automatic withdrawal of links to any objected contents or to an unmanageable number of requests handled by the most popular and important internet search engine service providers.'[14]

Google had argued that search engines do not distinguish between data protected by the DPD (personal data) and other data, and that furthermore it had no control over the data or its selection. At a national level, the argument presented was that Google was not a 'controller'[15] but rather was merely replicating the data and not involved with data processing. Consequently, Google considered that it did not 'determine […] the purposes and means of the processing of personal data' as required by the terms of the DPD. The CJEU rejected these arguments. The CJEU ruled a search engine operator is a data controller[16] as defined under Art 2(d) as 'it determines the purpose and means of the processing' of the data it collects and shares. It was not contested that the data contained therein was of a 'personal'[17] nature, as required by the DPD. It was said that 'a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of

search results.'[18] This would appear to be a broad definition being adopted as to the concept of a 'controller.'

The CJEU chose not to follow Google's argument or the A-G's line of reasoning where awareness and intent were critical characteristics of a data controller in relation to personal data posted on the Internet. It agreed that publication of personal data on a website constitutes processing. However, the CJEU had no doubt that the operations of a search engine themselves constituted processing of personal data regardless of the fact that such operations did not alter the personal data or distinguish it from non-personal data. In reaching this conclusion it considered the impact of the search engine on linking individuals to results. The CJEU concluded that:

> 'as the activity of a search engine is therefore liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.'[19]

Ultimately, the CJEU found each of Google's activities such as collecting and retrieving, storing data etc. to satisfy 'processing' regardless of the fact that it also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data. It ruled the automatic actions of a search engine fall squarely within the activities listed in the definition of processing in Art 2(b) of the Directive.

3.2. THE TERRITORIAL SCOPE OF THE DIRECTIVE, I.E. WHETHER IT APPLIES TO A SUBSIDIARY, GOOGLE SPAIN, GIVEN THAT THE PARENT COMPANY IS BASED IN CALIFORNIA, USA

When considering whether the DPD applied to Google, the CJEU considered two possible outcomes. The first was that Google's activities naturally fell within Article 4(1)(a) which applies the DPD to those with an 'establishment' in a Member State.[20] The second relates to Article 4(1)(c) which concerns the 'use of equipment situated on the territory of the said Member State.'

In arriving at its conclusion, the CJEU emphasised the purpose of the DPD and the need to protect privacy.[21] The CJEU considered that the use of advertisements in Spain could be seen to have satisfied the requirement that the processing be 'carried out in the context of the activities' of the EU establishment. The CJEU concluded:

> 'the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute

> the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.'[22]

The CJEU felt that the activities of Google Spain are, in reality, linked to the search function of its parent company, the processing therefore fell within Art 4(1)(a) because it was carried out 'in the context of the activities of an establishment of the controller' within a Member State. The DPD, in the manner implemented by Spain, applied. The CJEU declined from ruling on the other possibilities with regards to the scope of the Directive and so those issues remain open in respect of the internet. The CJEU did go as far as saying the rules on the span of the DPD 'cannot be interpreted restrictively', and that it had 'a particularly broad territorial scope.'[23]

3.3. THE RESPONSIBILITY OF SEARCH ENGINE OPERATORS

The CJEU stated that search engine operators are responsible, separate from the original webpage publishers, for removing information on data subjects from search engine results, even where the publication on the original news or webpages might be lawful.

The question became whether the complainant had the right to demand erasure, blocking or rectification when this was not on the basis of the data being inaccurate. The CJEU ruled that within the scope of the DPD there is a right to demand rectification where the processing was unlawful for other reasons, including non-compliance with any other ground in the DPD relating to data quality or criteria for data processing, or in the context of the right to object to data processing on 'compelling legitimate grounds'. The result being that individuals that are the subject of data could request that search engines erase personal data from their search results and if they were to refuse the request the data subject would have avenue of complaint to the supervisory authorities or courts on refusal.

Article 7(f) of the DPD provides that in some circumstances there can be a ground for processing data if it is in the legitimate interests of the controller. There would need to be no contract, public interest requirement, legal obligation or consent by the data subject for this ground to apply. In this case the court decided that here those interests were 'overridden' by the rights of the data subject. This necessitates a balancing exercise of rights – that of the public right to freedom of expression and that of right to privacy. Google raised the argument it had fallen under the ground of having a public and economic interest in the data being available. The CJEU stated that the huge impact on the right to privacy 'cannot be justified by merely the economic interest of Google as the search engine operator'.[24]

It is important to note that the CJEU drew a distinction between the operator of the website and a search engine. Stating that even if the continued processing of the data on the website was lawful, it does not follow that processing for generating search results will be lawful. It appears from the decision on this point, the greater impact of a search engine's results in an

even more stringent application of the test on the impact on the right to privacy. It goes beyond a mere balancing of the rights in such a case.

There then remains the possibility that a request for erasure could result in the information removed or blocked from the search engine whilst it remains available in full on the original website. The CJEU was clear on the view that search engines like Google cannot rely on the argument of 'journalistic'[25] exception from the Directive. Interestingly, this was an answer to a question not actually presented to the CJEU during the case.

3.4. THE CONCEPT OF THE 'RIGHT TO BE FORGOTTEN', I.E. THE RIGHT OF AN INDIVIDUAL TO INSIST (IN THIS CASE) THAT HIS OR HER HISTORY BE REMOVED FROM ACCESSIBILITY VIA A SEARCH ENGINE

The CJEU accepted the arguments that the DPD's requirements that data of such a personal nature must be retained for limited periods of time. It would only be for as long as it is relevant and that ultimately this amounts to a form of 'right to be forgotten.'[26] The CJEU left it to the referring national court to apply this right to be forgotten to the facts of this case which leads the national court to the conclusion that the data subject's rights had been violated.

The CJEU concluded that:

> 'as the activity of a search engine is therefore liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.'[27]

The decision has repercussions in terms of the applicability of EU law even to non-EU-based companies and the rights that individuals have against those processing their data. This is not limited to first publishers of material but those who republish – including search engines.

An interesting nuance of the decision was that the conclusion reached by the CJEU may have been different if there had been an interest of the general public having access to the information, such as where the data subject has a role in public life. If the personal data generated by way of search results is no longer relevant, or is excessive with respect to the purpose for which it was originally processed, the search engine operator must remove the material unless retaining the results is otherwise justified. It is not fully clear to where 'justification' extends.

The case is now returned to the Spanish National Court. The CJEU decision does not arguably go as far as establishing an individual's 'right to be forgotten.'[28] However, it is the requirement of those controlling the search engine to stop processing data upon receipt of a valid request from the data subject. Questions abound regarding how the search engine controller lawfully responds to that request.

4. IMPLICATIONS OF THE DECISION – AN ATTACK ON THE FREEDOM OF EXPRESSION AND THE RIGHT TO KNOW?

The CJEU has effectively ruled that Google acquires data protection obligations at the point that it collects the information from the Web. Google now finds itself having to respond to complaints from individuals[29] that their personal data, found as a result of a Google search, is too historical to arguably be of relevance any more, whether that information is inaccurate or not. Google can then be challenged further before a supervisory authority or in the national courts.

An issue with which data controllers such as Google will have to contend is with what other requirements they will need to comply from now on? Under EU data protection, it is possible Google could be obliged to provide privacy notices. Google has the challenge of treading a fine line when making what may be termed a difficult decision as to what amounts to 'inadequate and/or irrelevant' material. There is even the possibility that it will be considered as having a positive obligation to act as soon as it has information, as it is identified as a data controller at the point of receipt. This is arguably a departure from what people would traditionally view as within the operations and remit of a search engine.

The decision can be viewed as a clear acknowledgement of the reality of modern day internet use and the role of search engines as they deliver information to their users. Ultimately a search engine is going to deliver a more rounded and complete picture about a person's entire life, more so perhaps than a third party would be able to obtain through other avenues, and as a result risks greater intrusion. In the judgment[30] the CJEU referred to the Directive's 'objective,' or a specific provision, as being to 'ensure… effective and complete protection' of data subjects, but this phraseology is absent in the DPD reading.

4.1. SOCIAL NETWORKS / MEDIA

Whilst the ruling concerns search engines alone, it can clearly have wider implications. The relevance of it in respect of social networks needs careful consideration. If the search engine complained of is a non-EU subsidiary that sells advertising in a Member State as part of its Internet services, then on direct transposition of this case they will be regarded as falling under the remit of the DPD.

Prior to the CJEU's ruling, it was considered that social media may be limited from exposure to the adverse effects of the DPD. Twitter's operations were

based in the US which were arguably outside of the remit of both the domestic and EU laws, whilst Facebook, through its operations being delivered from its base in Dublin, was subject to the laws. However, given *Google v Spain*, both corporations are subject to EU data protection and privacy laws and, particularly given the nature of Twitter users' comments and re-tweeting information, the poster's of material which may constitute a criminal offence[31] or could later prove embarrassing, may wish for their removal. Users may be able to approach Twitter or Facebook (notorious for the difficulties in users being able to remove their accounts) to delete information posted about them rather than it remaining online indefinitely (and available through searches and re-tweets). Further, given Google's reported acceptance of requests to remove links to information, seemingly without much hesitation, it further provokes questions as to the likely winner in the privacy v freedom of expression battle. If Twitter and Facebook follow a similar passive route, and for the avoidance of further legal action and potential costs why wouldn't they, information may become more difficult to access, not because it is unavailable, private or sensitive, but simply because a form was completed and the search engine / source chose the path of least resistance rather than entering an argument with the data subject. Accuracy of the information, albeit potentially embarrassing for the data subject, is not seemingly at issue when the choice is made to remove the entry from future searches listings.

4.2. PRIVACY

There is an argument that the CJEU has overly concerned itself with the right to privacy and in enforcing it they have excluded the other rights applicable in such cases. In the case, the CJEU appears to have set an automatic test: if the individual data subject is not a public figure then their interest will override the economic interest of the search engine. It is worth noting that not every individual that has historical data online about him or her will choose to challenge this, it will most likely be those who feel some form of embarrassment/unease as to the data,[32] however that number could be significant. It is obviously less likely that an individual would seek to remove reports of positive achievements. The removal requests will probably focus on links to sites hosting unfavourable details of the individual.

Privacy is a significant concern to private individuals given the invasive nature of modern technology[33] (perpetuated in many cases by the person's own actions by submitting personal and professional material and data on various social media sites), the ubiquity of technology and information on demand, and the nature of information available through internet search engines which may 'live' for a much longer period of time and remain 'relevant' when a person's name is the subject of a search, compared with other media. Search engines further face a problem given the information which is returned. For other media searches, specific terms, issues, criteria or facts may need to be selected before information on that basis is provided. With Mr González, a simple search of his name gave the return of the embarrassing information regarding his financial situation near the top of the first page of search results. This result did not require any further and specific search criteria to be entered into the engine other than the individual's name. This clearly is

problematic given, first, González's status as a private individual, secondly, the limitation, in the UK at least, of any likelihood of successfully arguing a breach of data protection laws[34] or the award of damages for a failure to remove data,[35] and thirdly, the web has existed for many years on the basis that information is primarily publicly available and free – albeit with the personal costs to individuals who may not wish all data held about them to be so readily accessible.

Google was obligated to secure the effective and complete protection of the data subject's rights and freedoms as envisaged by the DPD.[36] The CJEU held that information on a search engine's results list 'makes access to that information appreciably easier for any internet user… and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page.'[37] This places a significant burden on Google as to protecting the data protection interests of individuals, and perhaps more surprisingly given the interaction between the EU and the EU Fundamental Rights Charter[38] and the European Convention on Human Rights,[39] the CJEU was silent on the balancing of rights and obligations between the individual's right to privacy / be forgotten and the fundamental right of freedom of expression. By implication, it appears that privacy trumps freedom of expression (unless the individual is a public figure / the information is in the public interest), but at what cost? The answer to that question will likely require years of judicial and legislative pronouncement, commentary and reasoning, however it is possible at this early stage to remark that the ruling imposes more stringent obligations on search engines than it does on the original website which hosts the published information. The search engines may not, held the CJEU,[40] rely on the journalistic exception within the DPD, although that is a defence available to the original publisher. There will be a difference in the obligations imposed on search engines compared with the information that is hosted and available on websites which appears odd and will need legislative action to provide direction and definition of the extent of obligations. The CJEU acknowledged[41] that the nature of internet search engines and the results pages provides an overview of personal data which may be widely used and causes concern for the person's privacy. However, given that the ruling does not require the original information or its original source / host to remove the information, it can only be seen as a worrying movement away from freedom of expression and freedom of information (freedoms which have been fought for and secured against increasing threats by governments of all persuasions).

A particularly important question to be answered is what amounts to a public figure? In the days of TV and the media making ordinary people celebrities through reality shows, it is increasingly difficult to see where the line will be drawn. This public interest aspect was narrowly construed. The CJEU appears to give little thought to the issue of freedom of expression – Article 11 of the EU Charter, Article 10 of the EU convention. The CJEU did not see it as being relevant or engaged in the case.

Many different interests are considered to be at stake here, with privacy being just one of them. Privacy appears to have won the first round, but there are likely more rounds to come with new cases. The operators of websites in the EU can potentially be drawn into protracted disputes over whether there is a specific public interest in the publication of the information under review, even where it is neither prejudicial nor private.

It will be important for the many players and users of the internet to watch how the decision is implemented in the future and it will be of interest to conduct research on whom become the primary take-down/erasure requesters over time. The question remains whether a supervisory authority could act on its own volition to enforce the judgment. On reading the case it would appear that the rights at issue are only those triggered by an individual complaining and so it is unlikely. Privacy campaigners may raise the issue of whether to introduce a human element to check through material, which is being indexed, prior to information being made publicly available.

An area of significance, unclear from the judgment, is the criteria to be satisfied when determining materials as 'historical'? How long will have to pass before the data is no longer relevant? If it relates to a debt, which has been paid in a short time and is no longer outstanding, the data subject may consider that historical on that basis but that may not be a sufficient passage of time as envisaged by the CJEU to satisfy this criterion. How will this be judged? Some data subjects may feel a greater level of embarrassment than others, over the same information. Will that have any bearing on the decision-making?

4.3. THE EXTENT OF THE RULING

Given the nature of the world wide web and internet searches generally, international jurisdictions can be problematic where information transmission is concerned. It has been suggested that Google is approaching the ruling by modifying the results of searches through 'EU versions' of its engine whilst individuals who make the positive choice of selecting the '.com' version will have full access to all, unfiltered, search results. It is also the case that preventing access to materials will not be prevented through this ruling, simply that the individual who wishes to discover information regarding a data subject may have to undertake a little more research than simply 'Googling' for an answer.[42] It is possible that Google may choose the simple route of filtering all results across its domains, not just applying the filters to EU-based versions of its engine, but this is more likely to be seen as overkill and unnecessary given the limitation to data subjects as search terms. Further, there will always be differing rules and interpretations on acceptable behaviour, offensive material, and the variances of public sensibilities between States. The facts of the case here involved a Spanish national, in Spain, being affected by a domestic rule regarding published material accessed through an internet search engine. Expanding the effects of removing direct access to the material regarding the individual from searches across the world seems unnecessary and counter productive. A 'one size fits all' mechanism would be unlikely to be effective, nor would this ever be desirable given the territorial / jurisdictional factors

involved. The *Google* ruling will affect searches in the geographical jurisdiction of the State concerned – but perhaps no further. Given the rationale for the ruling, that individuals (data subjects) should have the right, in limited circumstances, that information relating to them is not accessible through the search engine, does restricting the application of this decision to Google searches within the State in which he or she resides sufficiently provide the respect for privacy that is being sought? Will the consequence of the ruling result in a shift in the habits of users of Google to use the .com site in preference to their domestic domain,[43] and if so, will this have any effect on future EU and domestic legislative initiatives?

5. REFORM OF THE DATA PROTECTION LAWS

As mentioned above the DPD was established before Google had been created and the CJEU considered the relationship between the DPD, the Charter of Fundamental Rights of the EU and the existence of search engines. The CJEU interpreted the DPD's provisions in light of the fundamental rights and freedoms laid down by the Charter and went as far as stating that the requirements that derive from these Charter rights are implemented in various Articles of the DPD. Therefore, arguably, the CJEU interpreted the provisions of the DPD in a wide manner, utilising a purposive reasoning, but also suggesting that protection afforded in the DPD is in need of reform.[44]

So where does the European Commission go from here with its plans for reform?

> 'they will continue pushing for a speedy adoption of the data protection reform, including the reinforced and modernised Right to be Forgotten. The Commission expects search engine operators to further develop well-functioning tools and procedures, which ensure that individuals can request the deletion of their personal data when they are inaccurate, inadequate, or irrelevant or no longer relevant – under the control of competent authorities in particular data protection authorities.'[45]

The search engines that had previously been faltering in their support of the proposed reforms may now view it as an opportunity to limit any liability they might otherwise have following this ruling. We may see greater co-operation in negotiations, however this will be some time in the making, even with an increased impetus to address this matter.

We are fast approaching 1 billion websites[46] and whilst Google has been deemed an 'establishment' within the meaning of the DPD, other search engines may not pass the threshold to satisfy this test.

The judgment made it clear that privacy rights have to be balanced with other rights. The CJEU saw Google as having its only countervailing right as one of commercial interest. Google would appear to have fallen victim of its own success, for it seems that it is now operating under a greater degree of legal

obligation than it had foreseen. With newspapers and other online publishers, the position may be different. The competing right to freedom of expression is much stronger, as has been repeatedly emphasised by the European Court of Human Rights. The Strasbourg court has a longer track record in this area than its CJEU counterpart in Luxembourg; something to which the CJEU is likely to pay considerable regard when determining the balance between privacy and other rights. Newspaper archives could perhaps be said to be more similar in nature to Google's search service than the daily news. However, newspapers' archives have traditionally been widely seen as an important matter of public record and the arguments supporting them are very strong in a way which simply does not apply to Google. The CJEU found that there was something particularly invasive in the way Google collated information relating to individuals from across the Web. Arguably this does not apply in the same degree in respect of newspaper archives. The debate may progress to the propriety of the continued availability of old personal data in online newspaper archives.

5.1. THE UK'S RESPONSE

Most recently, a question raised by Lord Birt in the House of Lords questioned the Government's legislative intentions in light of the CJEU ruling. In a written response, [47] Lord Faulkes stated the Government was considering the implications of the ruling and that the work being undertaken by the Committee of European Data Protection Authorities to develop criteria to be used by search engine operators when considering requests for deletion, was being closely monitored. The guidance is needed by search engines operators to enable them to strike the right balance between the privacy rights of individuals and other interests, including the public interest in retaining the information.

Lord Faulkes further identified the negotiations on a replacement General Data Protection Regulation ongoing in the Council of the EU, including the proposed 'right to be forgotten' provisions. The Government opposes[48] the stance adopted by the Commission in relation to the 'right to be forgotten' as it wishes to avoid the pitfall of setting unrealistic expectations for data subjects which do not exist in practice (in part at least, due to the technological limitations in existence). The Government, further, considers that an obligation to inform other controllers of a request under the 'right to be forgotten' should be more transparent and proportionate. A potential conflict[49] between the UK, and the requirements of the European Union and being a signatory to the European Convention on Human Rights could be the result of the ruling and the UK's stance towards data protection and technological limitations.

6. CONCLUSION

If the extent of this case remains narrow, relating to a search engine, then the significance is clearly lessened, however the CJEU appears to have issued a ruling which has potential to be more far reaching. Only time will tell as to what its full implications are. The position in which we are left is data controllers potentially having to remove data which is sensitive and prejudicial,

and even going as far as a proactive duty not to release such material from the start. That is where the argument lies, but this would be a radical departure from the freedom of expression and the legal tensions between the convention rights and EU Treaty rights, not to mention the international dimension of possible reactions of companies based in the US / outside the EU complying with EU regulations.

---

[1] University of Huddersfield. The author would like to thank Michael Jefferson, James Marson, Prof. Philip Leith and the anonymous referee for helpful comments on drafts of this article. Errors and omissions remain my own.

[2] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, judgment 13th May 2014.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281, 23/11/1995 P. 0031 - 0050

[4] V. Mayer-Schonberger, 'Generational Development of Data Protection in Europe' in Philip E. Agre and Marc Rotenberg (eds.) Technology and Privacy: the New Landscape (Cambridge, MA:MIT Press, 1997), 232.5.

[5] http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[6] "Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century" COM(2012) 9 final.

[7] Opinion of Advocate General Jaaskinen delivered on 25 June 2013, para. 7.

[8]Case C-101/01 (Reference for a preliminary ruling from the Göta hovrätt): *Bodil Lindqvist*, OJ 2004 C7/3.

[9] Peter Hitchens 'The Superstar footballer, A Swedish Lady's Injured Foot… and a sinister threat to our freedom' The Mail on Sunday (LONDON) Jan 11 2004 at 72.

[10] Although of course, the fact that he brought this legal challenge likely means that the details of his financial history have become known even more widely.

[11] Agencia Española de Protección de Datos.

[12] Para 16 Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*.

[13] para 17.

[14] Opinion of Advocate General Jääskinen delivered on 25 June 2013 at [133].

[15] Article 2 of Directive 95/46 states that '[f]or the purposes of this Directive: "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

[16] The CJEU had previously ruled on this in Case C 73/07 *Satakunnan Markkinapörssi and Satamedia* [2007] ECR I-7075, paras 48 and 49 (in the context of tax information published on CD-ROM). It would appear that the definition of 'processing' does not require that the data be altered.

[17] Personal data held on a webpage is subject to the DPD (Case C-101/01 (Reference for a preliminary ruling from the Göta hovrätt): *Bodil Lindqvist*, OJ 2004 C7/3), although the case did not consider the use of search engines.

[18] paras 28-29.

[19] para 38.

[20] DPD '… in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States;.. in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;' Article 18.

[21] paras [53-54].

[22] para [56].

[23] para [54].

[24] para [81].

[25] para [85].
[26] para [91].
[27] para [38].
[28] At the moment, the search engine needs to take no action unless and until the data subject makes such a request to have links to source material removed.
[29] https://support.google.com/legal/contact/lr_eudpa?product=websearch - the form 'went live' on the 30th May 2014.
[30] at paras [34], [39], [58], and [84].
[31] See, for example, the instance of Liam Stacey and his comments on Twitter in 2012 regarding the footballer Fabrice Muamba who collapsed during the Tottenham Hotspur v Bolton Wanderers match. Stacey's comments, which were re-tweeted and caused due to their racist nature, resulted in a successful prosecution under the Public Order Act 1986 and his sentence to 56-days in prison.
[32] It should be noted that the case has demonstrated the 'Streisand Effect' – so called after the *Streisand v. Adelman* (2003), case number SC 077 257 judgment. Named after the American singer and actress Barbra Streisand, the Streisand Effect is now the accepted term for where attempts to achieve suppression of information made available online can backfire and result in actively publicizing the issue for the would-be censor. In 2003, Barbara Streisand sued the California Coastal Records Project on the grounds that an online archive included pictures of her Malibu mansion and she thus claimed an invasion of privacy. As the case became more well known, far more people than would otherwise have searched the archive accessed the pictures and consequently, by the end of the case, Streisand's privacy had been far more compromised than it would have been had she chosen not to pursue the case.
[33] Including the ease of access to materials.
[34] A complaint could be made to the Information Commissioner's Office.
[35] It may be possible for an individual to serve a section 10 notice on the basis of his/her 'objection to processing' personal data through the Data Protection Act 1998 s. 10.
[36] at [38].
[37] at [87].
[38] Article 11.
[39] Article 10.
[40] at [85].
[41] 'It must be pointed out at the outset that.., processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (see, to this effect, Joined Cases C□509/09 and C□161/10 *eDate Advertising and Others* EU:C:2011:685, paragraph 45).' [80].
[42] See http://www.techtimes.com/articles/9370/20140630/google-deletes-search-results-in-europe-abides-by-right-to-be-forgotten-rule.htm.
[43] e.g. - google.co.uk; .es; .fr etc.
[44] See Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data/COM/2012/010 final.
[45] http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_en.pdf.
[46] http://www.internetlivestats.com/total-number-of-websites.
[47] HL Deb 22 July 2014, Vol 755 col WA193.
[48] On the 30th July 2014, the House of Lords' EU Home Affairs, Health and Education Sub-Committee F released a report, articulated through its Chairman Baroness Prashar, finding 'We believe that the judgment of the Court (of Justice) is unworkable. It does not take into

account the effect the ruling will have on smaller search engines which, unlike Google, are unlikely to have the resources to process the thousands of removal requests they are likely to receive. It is also wrong in principle to leave search engines themselves the task of deciding whether to delete information or not, based on vague, ambiguous and unhelpful criteria. There are compelling arguments that, in the new Regulation, search engines should not be classed as data controllers. We do not believe that individuals should be able to have links to accurate and lawfully available information about them removed, simply because they do not like what is said. It is incredibly difficult for legislation to keep up or 'future proof' the unforeseen leaps that technology is bound to make. We do, however, need to ensure that the next Regulation does not attempt to give individuals rights which are unenforceable.'

[49] Although legally distinct, there is an interaction between the European Convention on Human Rights (European Convention) and the European Union (EU) (if, for no other reason accession to the European Convention was incorporated into the EU under the Treaty of Lisbon as of 1st December 2009). The rulings of the European Court of Human Rights (enforcing European Convention rights) and the European Convention provisions, transposed in the UK through the Human Rights Act (HRA) 1998, and the EU, and the rulings of the Court of Justice of the European Union, are interesting in relation to obligations on the UK. The HRA provides that the human rights contained in the European Convention form part of the law of the UK in the following ways: 1) The law of the UK must be interpreted, so far as it is possible to do so, in a way that is compatible with the HRA (s. 3); 2) Where an Act of Parliament breaches the HRA, the courts can issue a declaration of incompatibility (which does not affect the validity of the law) (s. 4) and 3) It is unlawful for any public authority to act incompatibly with the HRA (unless under a statutory duty to so act) (s. 6). It is quite possible for the UK to refuse to follow the provisions of the European Convention (as demonstrated in the Supreme Court in *R v Horncastle* [2009] UKSC 14; [2010] 2 WLR 47, following *Al-Khawaja and Tahery v UK* ((2009) 49 EHRR 1 – along with substantial commentary and justification from the departure with the European Court of Human Rights ruling: 'There will, however, be rare occasions where the domestic court has concerns as to whether a decision of the Strasbourg court sufficiently appreciates or accommodates particular aspects of our domestic process. In such circumstances, it is open to the domestic court to decline to follow the Strasbourg decision, giving reasons for adopting this course.' at [11]). However, principles of supremacy and doctrines of direct effect and the gamut of enforcement mechanisms of EU law, established through the rulings of the CJEU and given effect through the UK's accession statute - the European Communities Act 1972 – specifically obliges the UK to follow the law of the EU and adhere to the rulings of the CJEU. It is a matter of settled law that the UK does not possess a power to merely refuse to follow EU law because it considers the interpretation of the CJEU as incorrect. The CJEU is the EU's court of reference, a body specifically empowered to clarify matters of EU law and provide a mechanism for consistent interpretation across the 28 Member States. That the House of Lords' EU Home Affairs, Health and Education Sub-Committee does not agree with the CJEU's ruling does not empower it to refuse to follow the decision or enable it to legislate contrary to it.