

The “right to be forgotten” demonstrates the need for legislative coverage of internet data protection

By Democratic Audit

*The rise of social media, and the data gathering potential that it holds, have made the issue of online privacy increasingly prevalent, with citizens often unaware of what is being done with information they had previously assumed would be used responsibly. Commenting on a recent Court of Justice of the European Union case, **Claire Overman** argues that the need for legislative coverage of internet data protection has never been more sorely needed.*



Facebook connections worldwide, as of 2010 (Credit: Michael Coghalan, CC BY SA 2.0)

The Court of Justice of the European Union has recently handed down judgment in the case of [Google Spain SL and Google Inc. v Agencia Española de Protección de Datos \(AEPD\) and Mario Costeja González](#). It examined the provisions of the EU’s [Data Protection Directive](#) in order to answer several questions posed by the referring Spanish court regarding data protection; in doing so, it has established what many have hailed as “the right to be forgotten.” However, the judgment (perhaps understandably) fails to grapple with the nuances of this right’s definition. The result is that its ambit is uncertain.

The individual claimant in this case, Mr. Costeja González, complained that, when an internet user entered his name into Google Search, links would be displayed mentioning his name in relation to a real-estate auction connected with debt recovery proceedings. This auction had taken place 16 years earlier. The question for the Court in this case, amongst others, was whether a data subject could require the operator of a search engine to remove certain results displayed following a search of the subject’s name. More importantly, the question was whether this obligation to remove extended to links to web pages published lawfully by third parties and containing true information, on the basis that that information might be prejudicial to him, or that he wished it to be “forgotten” after a certain time.

The respondents, Google and Google Spain, argued that the Directive conferred rights on data subjects only if the processing in question was incompatible with the Directive, or on compelling legitimate grounds relating to their particular situation. According to them, it should not confer rights merely because the data subject considered that that processing may be prejudicial to him, or because he wished that the data being processed “sink into oblivion.”

The Court agreed with Mr. González. It noted that the lawfulness of data processing was not fixed, but fluid, stating that;

“Even initially lawful processing of accurate data may, in the course of time, become incompatible with the Directive where those data are no longer necessary in the light of the purposes for which

they were collected or processed.” More strikingly, it stated that for the “right to be forgotten” to be established, “it is not necessary that the inclusion of the information in question...causes prejudice to the data subject.”

Given the facts of the present case, the Court held that;

“Having regard to the sensitivity for the data subject’s private life of the information contained in those announcements and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that the information should no longer be linked to his name.” Further, it held that there were “no particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information.” It did, however, note that this interest was something for referring courts to establish, and gave guidance that such a public interest might exist due to the “role played by the data subject in public life.”

The response to this judgment has been mixed. There have been [reports](#) that it will lead to candidates for public office having “a means of curating their own bespoke search results.” However, this is surely the archetypal situation which the judgment, with its reference to information in which the public will have a “preponderant interest,” seeks to avoid. On the other hand, this definition is rather ambiguous. Who constitutes “the public,” and what is a “preponderant interest”? It may be that such data relating to historical debt recovery proceedings is precisely the type of information that banks seek to discover before granting credit.

Yet, following the facts giving rise to this judgment, it appears that such information may now be removed after a certain lapse of time. One could equally imagine a situation in which a public figure, such as a celebrity or politician, requested the removal of information identical to that at issue in the present case. Would the public have a “preponderant interest” in this information, merely by virtue of the data subject’s identity? Of course, it is perhaps as a result of its position as a supranational court that the CJEU defers these questions to national courts. Yet if one topic cries out for harmonising guidance at European level, it is surely internet data protection: such a medium of its nature transcends geographical boundaries.

This brings us to consider a further conceptual difficulty in relation to this type of data protection. The very reason that many wish for their data to be obliterated is that there are many others who may be interested in knowing about it. Inconsequential information about an individual appearing on a Google search is unlikely to be the subject of a data privacy action, precisely because it is of so little interest that it is not worth the time and expense in seeking its removal. Data which has the potential to cause a stir, on the other hand, is worth the expense of a legal challenge, at the same time as it may be of great interest to the public. A considered balancing of these competing interests is called for, if we are to establish principled limits to a right to removal of information.

It has been [suggested](#) that this judgment will lead to greater pressure to develop legislation specific to the demands of information-sharing online. It must not be forgotten that the Data Protection Directive pre-dated the expansion of the internet, and indeed, not one reference may be found to it within the text. Two problems therefore require resolution: the absence of legislation, whether domestic or European, tailored to the specificities of internet data protection; and the ambiguous scope of the “right to be forgotten.” The European Commission’s [2012 proposal](#) for a “comprehensive reform of data protection rules” will hopefully improve upon the present situation.

Note: this post represents the views of the author and not those of Democratic Audit. Please read our [comments policy](#) before posting. The shortened URL for this post is: <http://buff.ly/1gAk4o4>

Claire Overman is a BPTC student at Kaplan Law School, having studied for a BA and BCL at the University of Oxford and the Université de Paris. She is the Editor of [Oxford Human Rights Hub](#) blog.

