ARTICLE 19's Response to Google's Advisory Council

16 October 2014

INTRODUCTION

ARTICLE 19 is an international human rights organisation, founded in 1987, which defends and promotes freedom of expression and freedom of information worldwide. It takes its mandate from the Universal Declaration of Human Rights, which guarantees the right to freedom of expression and information.

ARTICLE 19 welcomes the opportunity to provide comments on the balance between the so-called 'right to be forgotten' (hereafter 'RTBF') and the right to freedom of expression online. Following *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014) (hereafter '*Costeja* judgment'), any person has the right to request Google and other search engines operating in the European Union ('EU') to remove links to results generated by a search for their name. The search engine will be required to remove those links in circumstances where the information is "inadequate, irrelevant or no longer relevant", regardless of whether or not the information provided in the third-party website is lawful.

In this submission, ARTICLE 19 not only sets out our concerns with the *Costeja* judgment but also seeks to provide practical guidance as to how search engines such as Google and data protection authorities should implement that judgment without prejudice to the ongoing negotiations of the Data Protection Regulation.[1]

Our submission is divided into three parts. Part I sets out our concerns with the decision for freedom of expression. Part II explains the traditional framework for balancing the right to privacy and freedom of expression, which data controllers and data protection authorities ought to follow when examining individual requests for delisting personal data from search results ('hereafter RTBF requests'). We also present what we consider to be the correct approach to specific categories of data, including archives, information about criminal proceedings and information published by governments.

Part III of the response makes a number of recommendations regarding the procedure that should be followed by data controllers and data protection authorities upon receiving RTBF

[1] Our comments are based on European human rights law as being most relevant to Google's request for comments on the way in which the *Costeja* judgment should be implemented. At the same time, our response should not be construed as ARTICLE 19's position on the broader right to be forgotten, which we will develop in a subsequent paper.

requests. These recommendations are designed to maintain a fair balance between the right to freedom of expression and the right to data protection in implementing the judgment. In addition, we suggest a number of steps that should be taken in order monitor the implementation of the judgment and ensure that the right to freedom of expression is protected in the transitional period leading up to the adoption of the General Data Protection Regulation.

I – ARTICLE 19's CONCERNS WITH THE *COSTEJA* JUDGMENT

1. The CJEU failed to properly take into account the right to freedom of expression

At the outset, it is clear that the right to freedom of expression was not taken properly into account in the *Costeja* judgment. Nowhere in its judgment did the CJEU refer to either Article 11 of the European Charter on Fundamental Rights or its equivalent under Article 10 of the European Convention on Human Rights ('ECHR'), notwithstanding its obvious relevance to the issue at hand. The Court's only reference to freedom of expression was not as a right but merely as an "interest" of the general public in "finding information", which as a "general rule" was overridden by the "rights" of the data subject under Articles 7 and 8 of the Charter (i.e. the rights to privacy and protection of personal data).

As the CJEU was interpreting the Data Protection Directive ('the Directive'), freedom of expression was merely considered as a narrow exception to data protection law rather than a right that had to be given equal weight in the balance of interests at issue. Indeed, under Article 9 of the Directive, data controllers may be exempt from their processing obligations in respect of personal data processed "*solely* for journalistic purposes or the purpose of artistic or literary expression". The exemption applies "*only if necessary* to reconcile the right to privacy and the right to freedom of expression". In our view, both the scope of the exception and the CJEU's application of it plainly failed to give proper weight to freedom of expression as a fundamental right.

While the CJEU and data controllers have recognised that the journalism exemption should be interpreted broadly[2] – which is welcome – the judgment has only served to highlight how the existing data protection framework has failed to recognise the broader scope of freedom expression, in particular those who express ideas and information for purposes other than journalism (e.g. academics) and those who are engaged in the dissemination of information (e.g. Internet intermediaries). In ARTICLE 19's view, this failing is all the more serious because of the ubiquity of data processing by computers and the increasing importance of such intermediaries in the digital age.

[2] See e.g. UK Information Commissioner, Guidance on Data Protection and Journalism, September 2014: http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data-protection-and-journalism-media-guidance.pdf

2. The judgment highlights that the data protection framework is inadequate to deal with the issues under the RTBF

We are further concerned that by holding search engines as data controllers for the purposes of the Data Protection Directive, the effect of the *Costeja* decision is to considerably and unreasonably broaden the reach of the protection of personal data beyond its original intended purpose.[3] In this regard, we note that the Data Protection Directive was adopted in 1995, i.e. before search engines even existed. While we accept that search engines pose serious challenges for the protection of the right to privacy and personal data online, we believe that the data protection framework is inadequate to deal with the wide range of new factual scenarios that arise in the context of their activities. In particular, it is obvious that the 'inadequate, irrelevant or no longer relevant' test was not conceived to address the practical issues that arise in the context of the RTBF. It is wholly unclear how search engines are to determine what personal data is 'inadequate', 'relevant' or 'no longer relevant' and to whom. If nothing else, it is apparent that there is no such thing as an objective conception of 'relevance'.[4] In requiring data controllers to assess the 'relevance' of information, therefore, the CJEU has set search engines an impossible task. We consider that, to the extent that the dissemination of inaccurate or private information may adversely affect a person's private life, it is better for such concerns to be dealt with by way of existing remedies under privacy and defamation law, rather than extending data protection laws in this way.

More generally, we are concerned about data protection being extended to areas that were previously not thought to fall within its ambit. In particular, it appears to us that the line between data protection, privacy and defamation is becoming unhelpfully blurred:

- **Data protection and the right to privacy**: whilst the right to data protection is widely understood as a subset of the right to privacy, [5] the scope of both rights is, in our view, significantly different. Whereas privacy generally protects information which is private, data protection concerns the protection of 'personal data' - i.e. data about a person - which may be both private *or* public. This is an important distinction, which presents serious difficulties in reconciling the protected interests where they diverge. This divergence is most obvious in the context of information which is already in the public domain.

- **Data protection and reputation:** in recent years, data protection law appears to be increasingly relied upon by individuals as a means to protect their reputations, either as an alternative for, or in addition to, the established principles of defamation law. The purpose of defamation, however, is to protect people against *false* statements of fact, which cause damage to their reputation, i.e. diminish the esteem in which other

[3] See Advocate General Opinion in the *Costeja* case, at para. 27: http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=EN

[4] The concept of 'relevance' itself is highly contested in Information Retrieval studies, see e.g. Lachica, Karabeg and Rudan, *Quality, Relevance and Importance in Information Retrieval with Fuzzy Semantic Networks:* http://folk.uio.no/dino/KF/Lachica-Karabeg08.pdf

[5] See e.g. http://www.out-law.com/en/articles/2013/november/data-protection-reforms-should-clarify-search-engine-responsibilities-when-privacy-take-downs-are-sought-/

members of society hold them.[6] By contrast, data protection laws enable individuals to request the erasure of information which is *truthful* so long as it is 'inadequate, irrelevant or no longer relevant'. The test is therefore easier to overcome and does not involve the defences normally found in defamation law. It may be that, in many cases, the journalism exception will prevent such actions against newspapers and the like. In our view, however, the scope of that exception is not an adequate answer to a development that seems to us to be wrong in principle. More generally, it is apparent that some courts are already beginning to elide the distinction between information which is 'irrelevant' and information which is defamatory. In a recent case, for example, the Court of Amsterdam held that the *Costeja* judgment was intended to protect individuals against 'being pursued' for a long time by 'irrelevant', 'excessive' or 'unnecessarily defamatory' expressions.[7]

- **The right to privacy and reputation**: like data protection, the right to privacy can be used to prevent the dissemination of accurate information of a personal nature, such as genuine photos taken surreptitiously in a private home. The effect that these facts have on the reputation of the person concerned is immaterial. Rather, the deciding factor is whether the plaintiff has proven wrongful intrusion into his or her privacy. Nonetheless, the European Court of Human Rights now regularly refers to a 'right to reputation' as an aspect of the right to privacy, despite the fact that the purpose of defamation laws and privacy laws are different.[8] Again, we are concerned that concepts that should properly be regarded as distinct for good reason are being unhelpfully muddled, which is made worse when data protection law concepts are thrown into the mix.

3. Search engines are not best placed to assess RTBF requests

Another unwelcome consequence of the *Costeja* decision is that search engines are now obliged to determine whether personal data is 'adequate, irrelevant or no longer relevant' and should therefore be de-listed. In our view, this is the kind of complex factual and legal balancing exercise involving the rights to privacy, free expression, and data protection that only a court should make, not private providers. In our view, the fact that search engines already remove links under the E-Commerce Directive is nothing to the point and indeed ARTICLE 19 has previously criticised such removals on similar grounds. Not only are private providers not equipped to carry out such determinations, but they also lack the necessary guarantees of independence and impartiality that individuals are entitled to expect whenever a decision affecting their rights to privacy and/or freedom of expression is made. In the absence of judicial determination of such questions in the first instance, freedom of expression is likely to suffer. In our view, individuals who wish to request the removal of links about them should therefore apply directly to the courts.

---

[6] See ARTICLE 19, *Defamation ABC* (2006), available here: http://www.article19.org/data/files/pdfs/tools/defamation-abc.pdf

[7] See C/13/569654, 18/09/2014, accessed from http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2014:6118

[8] See Hugh Tomlinson QC, *Privacy and Defamation: Strasbourg blurs the boundaries,* 23 January 2014: http://inforrm.wordpress.com/2014/01/23/privacy-and-defamation-strasbourg-blurs-the-boundaries-hugh-tomlinson-qc/

4. Data controllers and DPAs must operate within the human rights framework

Notwithstanding these concerns, we accept that the CJEU judgment is binding and that search engines operating in the EU are therefore required to implement its rulings. In our view, however, search providers must ensure that they do no more than is strictly necessary and – in particular – providers should take particular care to ensure that the right to freedom of expression – itself a fundamental right under EU law – is not unduly encroached. Consistent with the Advocate General's approach in the *Costeja* case, we believe that in determining requests for personal data to be removed from search results, both data controllers and data protection authorities should seek to strike a balance between the right to freedom of expression and the rights to privacy and personal data under the EU Charter of Fundamental Rights. In doing so, they should have regard to the jurisprudence of the European Court of Human Rights, which is well developed in this area. This would also mitigate the legal uncertainty and practical difficulties raised by the developments outlined above.

II - HOW TO BALANCE FREEDOM OF EXPRESSION AND THE RIGHT TO PRIVACY

The right to freedom of expression and the right to privacy are two fundamental, yet qualified, rights. Both may be limited subject to three conditions, namely legality, necessity and proportionality. As two equal human rights, they must be balanced in a fair and proportionate manner without giving precedence to one over the other. Furthermore, the European Court of Human Rights stated:

> The balancing of individual interests, which may well be contradictory, is a difficult matter and Contracting States must have a broad margin of appreciation in this respect since the national authorities are in principle better placed than this Court to assess whether or not there is a "pressing social need" capable of justifying an interference with one of the rights guaranteed by the Convention.[9]

In practice, the European Court of Human Rights has developed a number of criteria in order to resolve such conflicts on a case-by-case basis. In *Von Hannover v Germany (No. 2)* the Court set out five criteria relevant to balancing the right to respect for private life against the right to freedom of expression. They are as follows:

i. Whether the information contributes to a debate of general interest;
ii. The notoriety of the person concerned;
iii. The prior conduct of the person concerned and their relationship to the press;
iv. Content, form and consequences of the publication;
v. The circumstances in which the material at issue was obtained (e.g. photograph taken with a hidden camera).

ARTICLE 19 believes that when there is a conflict of interest between the RTBF (or data protection rights) and the right to freedom of expression, data controllers and data protection authorities ('DPA') should apply the above criteria in conjunction with the criteria already

[9] See *MGN v. the United Kindgom,* no.39401/04, 18 January 2011, at para. 142.

identified by Google as being relevant to the balancing exercise.[10] The overarching presumption, however, should be that information already in the public domain should remain in the public domain.

(1) The public interest should be broadly defined

In our view, the public interest is a concept which must be interpreted broadly to encompass information about public officials and public figures which is important to matters of public concern. This includes, but is by no means limited to, politics, public health and safety, law enforcement and the administration of justice, consumer and social interests, the environment, economic issues, the exercises of power, and art and culture.

We recognise, however, that it does not include purely private matters in which the interest of members of the public, if any, is merely salacious or sensational.[11] In particular, the ECtHR has clarified that it puts a higher value on information which would contribute to public debate rather than a lesser interest in merely providing to the public curiosity.[12] In *Mosley v United Kingdom*, the Court stressed that when assessing whether there is a public interest which justifies an interference with the respect for private life, the focus must be on whether the publication is in the interest of the public and not whether the public might be interested in reading it.[13]

(2) Public figures have a lesser expectation of privacy

At the same time, it is well-established under European human rights law that public figures, especially leaders of states and elected representatives, have a lesser expectation of privacy than private figures or even lesser officials. The more significant a public figure is, the more they should be subject to, and tolerant of, the highest levels of scrutiny in accordance with the principles of democratic pluralism.[14]

By extension, even if the information in issue has nothing to do with the persons' official duties, it may still be afforded protection under Article 10.[15] As noted by the Council of Europe Parliamentary Assembly, "*[c]ertain facts relating to the private lives of public figures, particularly politicians, may indeed be of interest to citizens, and it may therefore be legitimate for readers, who are also voters, to be informed of those facts".*[16] For example, the ECtHR ruled that the tax records of public figures could be published as a means of improving the public debate.[17]

---

[10] This includes whether the individual is a public figure; the source of information; how recent it is; whether it involves political speech; questions of professional conduct that might be relevant to consumers; the involvement of criminal convictions that are not yet "spent"; whether the information is being published by a government.

[11] ARTICLE 19, Defining Defamation: Principles on Freedom of Expression and Protection of Reputation, July 2000: http://www.article19.org/data/files/pdfs/standards/definingdefamation.pdf

[12] See *Von Hannover no. 2 v Germany*, nos. 40660/08 and 60641/08, [GC], 7 February 2012, at para. 110.

[13] *Mosley v The United Kingdom*, No.48009/08, 10 May 2011, at para. 114

[14] *Lingens v. Austria,* No. 9815/82, 8 July 1986

[15] *Karhuvaara and Iltalehti v Finland,* No. 53678/00, 16 November 2004

[16] Resolution no 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy

[17] *Fressoz and Roire v. France,* No. 29183/95, 21 January 1999

Nonetheless, public figures retain privacy rights in relation to those things which are done in private, that are not relevant to the individual's public activities and do not engage the public interest.

Furthermore, in *Axel Springer v Germany*, the Grand Chamber confirmed that there exists a right to protection of reputation under Article 8, subject to the following criteria: [18]

i. The attack on reputation must attain a "certain level of seriousness" and "in a manner causing prejudice to personal enjoyment of the rights"
ii. Article 8 cannot be relied upon to complain of a loss of reputation which is the foreseeable consequences of a person's actions.

In light of the above, we believe that in the case of RTBF requests submitted by public figures, there is a strong presumption that links to data should not be delisted from search results. Alternatively, and in any event, the inherent public interest in a public figure means the data in issue is highly unlikely to meet the "inaccurate, inadequate, irrelevant or excessive" threshold in the vast majority of cases.

3. Other categories of data

(a) Archives

Archives are essential to the preservation and appraisal of human culture and collective memory.[19] The European Court of Human Rights has recognised that the maintenance of Internet archives is a critical aspect of the role of the Internet in enhancing the public's access to news and facilitating the dissemination of information generally.[20] In relation to Internet news archives, the Court has gone even further and said:

> "[It was] not the role of judicial authorities to engage in the rewriting of history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations."[21]

Data protection authorities themselves consider that historical and cultural data – which may include personal data - are protected under freedom of information and "should be encouraged and treated as a valid way to retain data beyond their operational utility date."[22] In other words, a wealth of information is unlikely to be 'irrelevant' even after the passage of a substantial period of time, if only because access to certain personal data may remain relevant for historical or research purposes.

---

[18] *Axel Springer v Germany,* No. 39954/08, [GC], 7 February 2012, at para. 83
[19] See Committee of Ministers of the Council of Europe Recommendation No. R (2000) 13 on archive access policy and practice in Europe.
[20] *Times Newspapers Ltd v United Kingdom (Nos 1 and 2),* nos. 3002/03 23676/03, 10 March 2009, at para.27
[21] *Wegrzynowski and Smolczewski v Poland Application*, No. 3346/07, 16 October 2013, para. 65
[22] Contribution of the Belgian Data Protection Authority to the European Commission's consultation on the comprehensive approach to personal data protection in the European Union, Brussels, 2011: http://bit.ly/pINtNI.

At the same time, ARTICLE 19 considers that a better test than 'relevance' in the context archives is whether the disclosure of *sensitive information* could cause *substantial damage* or *harm* to the data subject. For example, in their Code of Practice on Archival Information, the National Archive of Scotland notes that the test of 'substantial damage' is not one of mere embarrassment or discomfort, nor is substantial distress sufficient, actual harm is also required.[23] For this reason, ARTICLE 19 believes that there should be a strong presumption that the provision of links to information contained in public archives should not be de-listed, unless the data subject can establish substantial harm that outweighs the public interest in direct access to that information, including by searching for their name.

(b) Personal information about criminal proceedings and law enforcement

Open justice is a central pillar of an open society. In our view, therefore, the publication and listing of information about criminal proceedings and law enforcement is inevitably a justified interference with the data-subject's right to privacy and his or her RTBF. This is consistent with a recent case concerning the right to be forgotten before the Court of Amsterdam. The Court of Amsterdam took a narrower approach to the RTBF or right to erasure, by reading into the CJEU's judgment the principles of 'being pursued for a long time' and 'unnecessarily defamatory'.[24] The court thus held that it would be hard for someone convicted of a *serious crime* to meet these criteria, as information about that individual would remain relevant. The court also considered the extent to which the claimant was seriously hindered in his private life as a result of the actions of Google.

We recognise, however, that the rehabilitation of offenders – and in particular spent convictions and juvenile offending – raises difficult issues in the context of the RTBF. In some jurisdictions, for example, juvenile offenders may exceptionally be given new identities in order to facilitate their rehabilitation while at the same time preserving the public record about their previous offending. Given the differing approaches of various Member States to this issue, we consider that the regulation of information about spent convictions is one better left to national authorities rather than seek to impose an EU-wide approach through the lens of data protection.

(c) Personal information published by governments

ARTICLE 19 notes that information held and published by government is a mix of public records, archives, personal information, copyrighted work, and other information. It includes criminal records, bankruptcy filings, court judgments as well publications such as Official Gazettes, which may contain personal information about individuals.

In the first instance, public authorities must always comply with data protection rules when taking any decision to publish material containing personal information. In the event that personal information is published, therefore, it is most likely because the public authority considered that, on balance, there was a greater public interest in the personal information being published in the first place. Even if this were incorrect, however, individuals who are

[23] http://www.nas.gov.uk/documents/dpaCodeOfPracticeOnArchivalInformation%20pdf.pdf
[24] See C/13/569654, 18/09/2014, accessed from http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2014:6118

aggrieved about the publication of such material would have a right of recourse to their national data protection authority.

In circumstances where personal information has been published by a government and, moreover, been in the public domain for some time, it would plainly be improper for such information to be de-listed under the RTBF. In our view, such a de-listing would constitute improper interference with the decision by a democratically accountable institution that was made in the public interest. Unless national legislation provides for the information to be expunged after a certain period of time, there is a strong presumption that the information should not be de-listed.

(e) Reviews of Professional or Consumer Services

ARTICLE 19 believes that there should be a general presumption that reviews of professional or consumer services should not be de-listed. Indeed, customer reviews inevitably reflect individuals' opinion as to the quality of products or services they receive. As such, they are a form of protected expression under Article 10 ECHR and Article 11 of the EU Charter. Delisting links to reviews of professional or consumer services therefore clearly interferes with the right to receive and impart information.

Moreover, ARTICLE 19 notes that delisting reviews is likely to raise another two sets of issues. First, it may engage Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market.[25] Delisting reviews of professional or consumer services arguably amounts to a misleading omission, per Article 7, which states:

> "A commercial practice shall be regarded as misleading if, in its factual context, taking account of all its features and circumstances and the limitations of the communication medium, it omits material information that the average consumer needs, according to the context, to take an informed transactional decision and thereby cause or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise."

Secondly, delisting data may have implications in relation to liability under tort law. It is arguable that a data subject who persuades a data controller to delist data linked to a website, may in fact be inducing the data controller to interfere with a business expectation, such as advertising revenue, between a third party publisher and the data controller and/or a third party publisher and an advertiser. In order to establish tortious interference, the claimant (the third party publisher) must show that the defendant (the data subject) had no legal justification or privilege for acting in a way that would harm or destroy the business relationship. Any de-listing requests, which are granted but successfully appealed, may therefore make the data subject potentially liable under tort law.

[25] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:en:PDF

III- PROCEDURAL SAFEGUARDS FOR THE PROTECTION OF FREEDOM OF EXPRESSION

1. Data publishers must be notified and be able to challenge RTBF requests

ARTICLE 19 notes that in practice, the procedure used to give effect to the RTBF presents similarities with notice-and-takedown mechanisms ('NTD') under the E-commerce Directive ('ECD'). Both place search engines in a position to decide whether access to content - or in the case of the RTBF, links – should be restricted. At the same time, the shortcomings of NTD procedures are well known: they lack both clarity and fairness.[26] In particular, individuals whose content is removed are not systematically informed that a request has been made to takedown their content in the first place. They are therefore unable to challenge them.

While we generally do not support notice-and-takedown procedures for the reasons outlined above, we recommend that in order to be maximally compatible with the right to freedom of expression, individuals should be both notified that a request to de-list their content has been made and given an opportunity to contest the request. If their content is de-listed, they should be given a right of appeal. A RTBF process compatible with these principles would therefore be as follows:

1) Once a RTBF request has been submitted by a data-subject, the data controller should make a preliminary assessment as to whether the request meets the formal requirements, whether the claim has prima facie validity.
2) If these criteria are met, the publisher of the data in issue should be given notice of the request and the opportunity to submit a counterclaim.
3) The data-controller would then be able to make an informed decision based on the evidence submitted as to whether the data is "inaccurate, inadequate, irrelevant or excessive" for the purposes of data processing, taking into account the broader human rights framework outlined above.
4) If the data is de-listed, the data publisher should be able to appeal the decision to the national DPA or preferably the courts.

We further note that the above notification requirement - as well as the possibility of appeal - is consistent with a range of international standards, including not just the Ruggie Principles on Business and Human Rights,[27] but also the requirement on member states under European human rights law to take positive measures to protect fundamental rights, including as between private parties. Although this principle underpins data protection law, we submit that it is equally applicable to the protection of freedom of expression. To the extent that data controllers may interfere with individuals' right to receive and impart information, the law should provide those individuals with an effective remedy.

[26] UN Special Rapporteur on freedom of expression, HRC/17/27, 16 May 2011, available here: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[27] See A/HRC/8/5, para. 92: http://www.reports-and-materials.org/sites/default/files/reports-and-materials/Ruggie-report-7-Apr-2008.pdf accessed on 10/09/2014

2. The RTBF request form should be improved

ARTICLE 19 is concerned that the vagueness of the 'inadequate, irrelevant or no longer relevant' test, coupled with the lack of guidance given by the CJEU in the *Costeja* judgment, effectively creates a procedural bias in favour of the RTBF over the right to freedom of expression. Accordingly, ARTICLE 19 suggests that Google's RTBF request form should be amended to include more probing questions and free text fields to elicit more comprehensive answers. For instance, the form used by Bing asks data-subjects to describe their role in society or the community, whether they are a public figure or celebrity, whether they have a role or expect to have a role which involves leadership, trust or safety (for example, teacher, clergy, community leader, police, doctor etc.).[28]

In addition, ARTICLE 19 believes that more stringent measures should be implemented to verify the identity of the data subject.[29] Data subjects should be required to adduce formal documentation or photographic ID in order to verify their identity. Such measures would go some way to ensuring the RTBF is not used in bad faith by private citizens, businesses or corporations trading under an individual's name.

3. Internet users should be able to request access to delisted data if they can show that it is a matter of public interest

What is of interest to the public is not a static concept and treating it as such could have a disproportionate restriction on the freedom of expression. As Jonathan Zittrain notes, "the ECJ decision says, something formerly relevant could become irrelevant, but the opposite is also true: something irrelevant could become relevant, such as when a private figure becomes a public one."[30] We concur. For this reason, we suggest that Internet users should be given the opportunity to request that previously de-listed information should be re-listed in order to give effect to their right to receive information under Article 11 of the EU Charter and Article 10 ECHR. This could be achieved by supplying an additional form where Internet users would be required to explain why they believe that the information they are seeking is now a matter of public interest. In order to make this right effective in the first place, search engines would notify Internet users that the search terms and links they are looking for have been de-listed. This could be done in the same way as Google is currently notifying users that some name-based search results may have been de-listed.

To the extent that this procedure would require the recognition of an actionable right to freedom of expression against data controllers, we reiterate that Member States are required to take positive measures to protect the rights and freedoms guaranteed in the European

[28] See Bing RTBF request form: https://www.bing.com/webmaster/tools/eu-privacy-request

[29] As noted by Michael Backes et al, the "definition of Data Subject is quite broad making the level of certainty required to identify the data subject unclear." Michael Backes, Peter Druschel & Rodica Tirtea, *The Right to Be Forgotten – Between Expectations and Practice,* EUR. NETWORK &INFO SEC. AGENCY 6 (Nov. 20, 2012) available at: http://www.enisa.eropa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten

[30] Jonathan Zittrain, 'The Ten Things that Define You', The Future of the Internet and How to Stop it Blog, 15 May 2014: http://blogs.law.harvard.edu/futureoftheinternet/2014/05/15/the-ten-things-that-define-you/ accessed on 10/09/2014

Convention on Human Rights. There is no principled reason why this requirement should not apply to the protection of freedom of expression vis-à-vis third-parties. By extension, the same principles apply to the EU Charter.

Alternatively, we recommend that delisted data should be subject to an expiration period or at least periodical review.

4. Search engines must publish statistics on RTBF requests in transparency reports

ARTICLE 19 is concerned that at present there are many disincentives not to refuse de-listing requests. Contrary to Google's assertion in answer to the Article 29 Working Party questionnaire, ARTICLE 19 believes economic interests are highly likely to have a chilling effect on the right to freedom of expression. This is especially so in light of the draft General Data Protection Regulation in its current form, which provides for an administrative fine of up to 5% of annual worldwide turnover of an enterprise for non-compliance with the Regulation's provisions.[31] We note that no such sanction is proposed for delisting data carelessly or excessively. We believe that data-controllers are much more likely to de-list links to pre-empt accusations of mishandling personal data as a result.

For this reason, it is vital that implementation of the judgment is closely monitored, the de-listing procedure and criteria being applied are transparent, and information about RTBF requests published. Transparency and accountability will be fundamental to ensuring that search engines' economic interests do not distort the balancing exercise between the RTBF and the right to freedom of expression. In particular, we believe that Google and other search engines should publish sufficiently detailed information about the nature, volume and outcome of de-listing requests. In our view, this could easily be achieved by adding a 'RTBF requests' category to search engines' transparency reports.

5. A code of practice should be developed through multistakeholder consultations

ARTICLE 19 believes that a publically available Code of Practice would help internet users understand the decision making process and assist data controllers faced with ethically complex requests. In this regard, we note the decision of the Article 29 Data Protection Working Party to put in place a network of dedicated contact persons in order to develop common case-handling criteria to handle complaints by the data protection authorities. It is anticipated that this network will provide the authorities with a common record of decisions taken on complaints and a dashboard to help identify similar cases as well as new or more difficult cases.[32]

ARTICLE 19 welcomes this move as a step in the right direction. We believe that it is entirely appropriate for the Article 29 Working Party to take the lead in developing a code of practice

[31] European Parliament Amendment 188, Proposal for a Regulation Article 79, adopted 12 March 2014.: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN

[32] Press release by the Article 29 Data Protection Working Party, Brussels, 18 September 2014, accessed from here: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140918_wp29_press_release_97th_plenary_cjeu_google_judgment__17sept_adopted.pdf

or practical guidance as to the way in which the *Costeja* judgment should be implemented. At the same time, ARTICLE 19 would welcome a more inclusive consultative process, involving search engines and other relevant stakeholders. In this regard, ARTICLE 19 would encourage data protection authorities to carefully consider the report of Google's Advisory Council on the right to be forgotten in developing guidance.

6. An independent public authority must supervise implementation of the judgment

ARTICLE 19 believes that in order to guarantee proper implementation of the judgment, an independent body, such as data protection authorities or information commissioners, should maintain a public database with records of de-listing requests in the same way as websites such as http://hiddenfromgoogle.com or https://www.chillingeffects.org. This would keep Internet users informed of the types of links that may be de-listed under the RTBF and enable data protection authorities and courts to hold data-controllers accountable for any arbitrary takedowns. It would also help ensure that data controllers' decisions are both objective and consistent.

Gabrielle Guillemin
Senior Legal Officer
ARTICLE 19