UNIVERSITY OF CAMBRIDGE
Faculty of Law

Dr David Erdos
Deputy Director, Centre for IP and Information Law
University Senior Lecturer in Law & the Open Society
WYNG Fellow in Law, Trinity Hall

Response to Guidelines 5/2019 on the Criteria of the Right to be Forgotten in the Search Engine Cases under the GDPR (Part 1)

Securing workable, balanced and effective individual rights regarding personal data disseminated online is vital to the future of data protection and should be a significant focus of attention for the European Data Protection Board going forward. Consequent to the Court of Justice's C-131/12 *Google Spain* (2014) judgment, the right to delisting and related *ex post* action by search engines has assumed particular practical importance. The European Data Protection Board (EDPB)'s draft guidance on this topic is, therefore, very welcome. Nevertheless, it is also important that in due course much more comprehensive guidance is produced. Indeed, under the General Data Protection Regulation (GDPR), the EDPB has a specific legal duty to *"issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services".*[1] This guidance will clearly need to encompass a much wider range of online actors than just search engines including individual websites, social networking sites such as Facebook and other online platforms such as Twitter. Nevertheless, it is recognised that the current Guidelines will be limited to search engines and so set out below are more detailed thoughts on this draft divided as follows:

(1) the scope of guidance and of *ex post* rights vis-à-vis search engines,
(2) the substantive grounds for exercising these *ex post* rights,
(3) the substantive exemptions from these *ex post* rights.

1. Scope of Guidance and of *Ex Post* Rights vis-à-vis Search Engines:

Once completed by the detailed criteria which will be set out in Part 2, these Guidelines seek to provide a general overview of the applicability of *ex post* rights vis-à-vis search engines as regards their indexing of personal data published online. This is put under the heading of the 'right to be forgotten' (RtbF) which is often used in public debate as a catch-all for rights to restrict to dissemination of personal data especially online.[2] Nevertheless, the Guidelines quite rightly also distinguish this use from the specific and new addition of a formal RtbF in Article 17 of the GDPR. Article 17 details the RtbF alongside the right to erasure. However, the addition it makes compared with the Data Protection Directive - which only used the language of the right to erasure - is to require those who have been subject to a bona fide erasure request *and* who have made this this public to help the data subject limit its further spread by others (GDPR, art. 17(2)). As the guidance points out, this provision has no applicability in relation to search engines indexing as they are merely processing personal data which has already been made public by others. It is also important to note that the right to erasure (which is sometimes itself called the RtbF) is not the only *ex post* right which may be invoked against search engines. Indeed, the *Google Spain* judgment itself emphasised that the right to object (now found in GDPR, art. 21) is equally applicable. Also of potential relevance are possibility of direct enforcement of the basic duties of data protection especially as set out in chapter II of the GDPR (through, for example, the data subject lodging a complaint with a Data Protection Authority under GDPR, art. 77), invoking of the right to restrict processing (GDPR, art. 18) and/or invoking of the right to rectification of inaccurate or incomplete processing (GDPR, art. 17). None of these provisions has been subject to detailed Court of Justice exploration and all must be interpreted in line with freedom of expression and, in particular, permissible exemptions applicable to the special data category rules (GDPR, art. 9(1)(g)), the criminal-related data rules (GDPR, art. 10) and the more general restrictions permissible where necessary to protect the *"rights and freedoms of others"* (GDPR, art. 23(1)(i)). Nevertheless, none can be entirely ignored and so they should at least be mentioned in

[1] GDPR, art. 70(1)(d).

[2] For a general discussion of various meanings ascribed to the 'right to be forgotten' online see section two of the following working paper: David Erdos and Krzysztof Garstka, 'The "Right to be Forgotten" Online within G20 Statutory Data Protection Frameworks' (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3451269

Trinity Hall
Trinity Lane
Cambridge
CB2 1TJ

any final Guidelines. Indeed, the potential relevance of the right to rectification has been highlighted by *C-136/17 GC et. al. v CNIL* which held that, in cases where a delisting of data is not applicable, a search engine is

> *in any event required, at the latest on the occasion of the right for de-referencing, to adjust the list of results in such a way that the overall picture it gives the internet user reflects the* [individual's] *current legal position, which means in particular that links to web pages containing information on that point must appear in first place on the list*.[3]

Incidentally, the Court's reference to *"at the latest on the occasion of the right for de-referencing"* suggests that in some circumstances a search engine may even have certain *ex ante* 'duty of care' responsibilities. For example, if a search engine's attention is repeatedly drawn to its indexing of a website dedicated to the publication of dissemination of manifestly illegal revenge pornography, then does it acquire a 'duty of care' responsibility under the GDPR to deindex this illegal material even before specific contact by each and every individual? These are important questions to pose but given the focus of the Guidelines on *ex post* duties they will only be noted here.

Turning back to consider these *ex post* duties further, the *Google Spain* judgment indicated that search engines would only acquire direct duties under data protection where their activities are *"liable to affect significantly and additionally"* the fundamental rights to privacy and the protection of personal data and would then only need to act with the framework of their *"responsibilities, powers and capabilities"* (at [38]). It is not entirely clear where the Court saw the grounding of these restrictions, as they do not obviously follow the logic of statutory European data protection scheme and yet the need for a proportionate balance with freedom of expression was also not argued for here either. Nevertheless, this language was repeated in the much more recent case of *GC et. al. v CNIL* (at [37]) – a judgment which did give some emphasis to freedom of expression - and so should be taken to be good law. [4] Nevertheless, notwithstanding the approach adopted by large search engines to date, name-based searches are only a *"particular"* (*GC et. al. v CNIL* at [46]) rather than the only example of processing which clearly satisfies the first threshold. Processing by reference to other widely used identifiers such as an image or a job position may also be significantly and additionally impactful on rights. Indeed, as regards the first example, the Article 29 Working Party highlighted as far back as 2008 that image processing may be particularly impactful and require specific attention.[5] Meanwhile, the latter type of identifier has even been subject to recent concrete enforcement action by the Italian Data Protection Authority (DPA).[6] Albeit only in certain restricted circumstances, it may even be possible for search engine activity to be significantly and additional impactful where its processing is not even by reference to a clear identifier. An example might be the enabling of search which combined reference to a small hamlet and a highly stigmatic allegation - e.g. being a "convicted child sex offender" – which brought up totally false details alleging that a identified person within that neighbourhood was responsible for such offences. The ability of anyone interested in the hamlet to readily find and potentially believe this false allegation would clearly have the potential to be highly damaging to such an innocent individual and additionally so compared with initial publication. This example goes to show the importance of ensuring that individuals are able to make a case to a search engine that the processing is significantly and additionally impactful on their rights and for both the search engine and on appeal the DPA to fairly consider it according to the standard laid down in CJEU case law. Obviously, and as with the analysis of name-based searches, any such claim must be interpreted consistently with freedom of expression including a search engine's right to facilitate communication by original publishers and the right of internet users to receive information. This will be dealt with further below. Nevertheless, parts of the guidance which seem to assume that only name-based searches are within scope should be deleted[7] and the initial part of the Guidelines which do to some extent recognise the need for a broader analysis made more complete and systematic.

It has been universally accepted that the second threshold - acting within the context of *"responsibilities, powers and capabilities"* – requires search engines to deindex specific URLs which are brought

---

[3] C-136/17 *GC et al v CNIL* at [78].

[4] Any such restriction is, however, without prejudice to duties which a search engine may have under, for example, the secondary liability law of Member States to bring its processing in compliance with law including data protection law where it is shown (for example, by a court injunction) that the dissemination of the data even by the original website is illegal. This liability does not necessarily even depend on a search engine being considered a 'controller'. See C-40/17 *Fashion ID* at [74].

[5] EU, Article 29 Working Party, *Opinion 1/2008 on Data Protection Issues Related to Search Engines* (2008), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf, p.. 14

[6] See Italy, Garante Privacy, Provvedimento del 20 giugno 2019 [9124401] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124401

[7] For example, on page 14 where it is currently stated that *"the effect of delisting is only that some results are deleted from the results page that is obtained when a name is entered as a search criterion".*

to its attention by data subjects and whose continuing processing is shown to violate core data protection standards. This is certainly an important minimum requirement. However, it has proved insufficient for individuals who may be faced with regular and repeated uploads of the same problematic personal data and which, thereby, leads on automatically to continuously impactful indexing which is not in conformity with core data protection standards. The criteria set down in *Google Spain* suggests that, once put on notice that such impactful and problematic indexing is taking place, search engines should have a responsibility to bring it into compliance with data protection standards as far as their *"powers"* and *"capabilities"* allow. Notwithstanding the resistance of major search engines on this topic, this may well extend beyond the bare deindexing of specifically notified URLs. For example, where the listing of certain images (e.g. manifest revenge pornography) is *ipso facto* of data protection standards, then the major search engines possess PhotoDNA technology enabling them to ensure that indexing of such images ceases. Following notice, this should therefore be deployed. In this regard, it should be noted that courts and regulators have recognised this as an issue to confront but that relevant cases have been settled[8] and so the required obligations remain opaque. This makes it all the more important that clear understandings are laid down in these Guidelines.

Finally, one responsibility which search engines clearly have is to ensure that they adopt all reasonable safeguards to ensure that own processing of deindexing claims does not either directly or indirectly lead to systematic processing which violates the purpose compatibility and/or associated legality standards to which they are bound. In reality, at least Google's practice of essentially blanket[9] and unsafeguarded disclosure of deindexing claims to original publishers has led to the data subject's claim, including its link with the underlying data at issue, being made public (sometimes even in combination with other private data such as claims an individual has made to self-regulatory bodies).[10] Under the necessity and other data protection standards which bind a Google and other search engines, the identifiable disclosure of deindexing claims to original websites should only take place where this is at least reasonably necessary for the purpose of determining or checking legal need for any deindexing. Even more importantly, any such disclosure must be subject to robust and effective safeguards to ensure that the disclosed data is not used for incompatible purposes which would include making public the data in identifiable form. The current draft of the Guidelines do mention this issue but is all too brief and, unlike the Working Party's 2014 Guidelines, they fail to mention the requirement in any case to *"take all necessary measures to properly safeguard the rights of the affected data subject"*.[11] In contrast to these earlier Guidelines, the new draft also fails to highlight that it would also be incompatible with data protection for a search engine to itself arrange for deindexing claims to be made public in identifiable form. Given the relationship between Google and the US-based Lumen database over recent years, the suggestion that Google might start disclosing deindexing data to Lumen and Lumen's usual practice of publishing 'removal' claims to the world at large, this is certainly an unfortunate gap.[12]

---

[8] As regards Courts see, for example, *Hegglin v Google* [2014] EWHC 2808 and *Mosley v Google* [2015] EWHC 59 (QB), both cases were settled. Meanwhile, albeit in the context of a social networking site rather than a search engine, the ICO expressed an interest in intervening in a case where a teenage plaintiff facing the repeated upload of revenge pornography was seeking to require Facebook to deploy PhotoDNA blocking technology. See "Data protection watchdog could feature in 'naked teen picture' Facebook legal action' (24 November 2016), http://www.irishnews.com/news/2016/11/25/news/data-protection-watchdog-could-feature-in-naked-teen-picture-facebook-legal-action-800632/. This case was also settled before full trial.

[9] Google has adopted policy of not disclosing such data to those who are running revenge pornography websites. However, no other general limitation has been publicly announced.

[10] See, for example, Greenslade, Roy, "Man who wished to be forgotten is remembered after Google Complaint", *The Guardian*, 4 July 2014, McIntosh, Neil, "December 2019: List of BBC web pages which have been removed from Google's search results", https://www.bbc.co.uk/blogs/internet/entries/98505970-e8f1-462a-8862-bc3187d6bf05 and Duffy, Nick, "BBC stars to crystal meth in anus: 19 PinkNews stories people want the internet to forget" (2 February 2016), https://www.pinknews.co.uk/2016/02/02/bbc-stars-to-crystal-meth-in-anus-19-pinknews-stories-people-want-the-internet-to-forget/

[11] EU, Article 29 Working Party, *Guidelines on the Implementation of Google Spain* (2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf, p. 10.

[12] I have provided a comprehensive analysis of these issues in a recent working paper including elucidating (in section four) why the notification duties set out in Article 17(2) and also Article 19 of the GPDR do not authorise, let alone require, such disclosures. See David Erdos, 'Disclosure, Exposure and the "Right to be Forgotten" after *Google Spain*: Interrogating Google Search's Webmaster, End User and Lumen Notification Practices' (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3505921. It should also be noted that according to this analysis an original website would also not be obliged to disclosure personal data to e.g. a search engine where it has been specifically asked by the data subject not to. This point should be clarified in the discussion at the top of page 7 of the Guidelines.

2. Substantive Grounds for Exercising *Ex Post* Rights vis-à-vis Search Engines:

The current draft of the Guidelines provides a very comprehensive analysis of the grounds upon which an individual may seek to exercise the right to erasure (GDPR, art. 17) against search engine processing. However, coverage of the potential relevance of other specific data subject rights is too limited and some of the detail of the analysis which is provided could also be improved.

Turning first to consider the grounds for exercising the right to erasure, the notion of personal data being *"unlawfully processed"* (GDPR, art. 17(1)(d)) should be construed so as to ensure effective and complete protection for the data subject and, in particular, that as far as possible a clear remedy is provided for infringement of any relevant duty which the GDPR requires (which, in relation to search engines, are at least all those set out in chapter II). As regards the four-corners of the GDPR, this concept should not therefore be limited to Article 6 of the instrument, which merely provides one mandatory element of lawfulness. Indeed, it is notable that in *Google Spain* itself there was as much emphasis on the core data protection principles now set out in Article 5. The data protection principles were also central to the way in which the much more recent case of *GC et. al. v CNIL* assessed the processing of past criminal proceedings. It would be particularly strange if a data subject was able to rely on a legal provision which was not even set out in the GDPR (as the Guidelines currently clearly state) but not on a breach of duty found not within Article 6 but, say, others parts of chapter II. Of course, all these duties and indeed the exercise of data subject rights must be construed consistently with freedom of expression (including its sub-right of freedom of information) and in line with the derogations established under Articles 9(1)(g), 10 and 23(1)(i) (see above). Indeed, it is notable that the Court in *GC et. al. v CNIL* held that the sensitive data derogations set out in Articles 9(1)(g) and 10 should be construed to be self-executing in the absence of implementing law enacted at national or Union level. The same should be true of Article 23(1)(i), the overarching *"rights and freedoms of others"* derogation. It should, however, be clear that even if the right to erasure itself is restricted in some way under Article 23(1)(i) it will remain necessary for the data subject to retain an ability to ensure that, where an infringement of the data protection principles of Article 5 or the legal grounds for processing in Article 6 are demonstrated, processing is brought into compliance with these standards. A purported derogation which makes this impossible would therefore not be compatible with the standards Article 23(1)(i) itself lays down.

Secondly, contrary to the suggestion in the draft Guidelines, it seems very doubtful whether the ground relating to the direct provision of information society services to a child (GDPR, art. 17(1)(f)) is in fact engaged since the child does not have a direct interface with the search engine but only with another online service such as a social networking site. Nevertheless, it is useful to highlight that a child's interests must be granted particular weight in any deindexing claim (see, in particular, GDPR, recital 38 and article 6(1)(f)).

Thirdly, many of the other applicable legal grounds for erasure are in essence elucidations of the overarching legality principle set down in Article 17(1)(d). Thus, if processing by a search engine is *"no longer necessary"* (GDPR, art. 17(1)(a)) it will also violate Article 6(1)(e) and so its ongoing processing will not be authorised. Similarly, if data have to erased in compliance with a legal obligation (GDPR, art. 17(1)(e)) then ongoing processing will also clearly be unlawful. These perhaps somewhat esoteric points aside, the analysis of these other provisions in the draft Guidelines are helpful.

Fourthly, the draft Guidance is right to recognise that the right to erasure may be triggered by a *bona fide* exercise of the right to objection (GDPR, art. 17(1)(b)). In principle, data subject rights including the right to object can be restricted in order to protect the rights and freedom of others under Article 23(1)(i). However, especially in the context of potential self-enforcement of any restriction rather than the enacting of specific legislation at Union or Member State level, it seems unlikely that a court would see any direct limitation of this right here as complaint with the required standards of respect for the essence of the right, necessity and proportionality in a democratic society. Nevertheless, the right obviously must be interpreted in line with the rights set out in the *EU Charter* including the right of a search engine to facilitate communication by original publishers and the receipt of information by internet users.

Finally, the draft Guidelines are also correct to note that, independently of the right to erasure, the right to object can itself be used to ground a claim to deindexing. Indeed, Article 21(1) specifically states that the successful exercise of the right to objection must result in the controller *"no longer process[ing] the personal data".* Moreover, given that deindexing generally focuses on a particular processing operation (e.g. a name-search or an image-based search), the exercise of a *"right to object"* to specific *"processing"* appears particularly apposite. Moreover, and as previously mentioned, whilst not explored in Court of Justice case law to date, it is also difficult to argue that the right to rectification of inaccurate or incomplete data (GDPR, art. 16) and the right to request a restriction of processing (GDPR, art. 18) should not have any application here. They, therefore, deserve a mention. Nevertheless, the balance with freedom of expression (and information) is particularly delicate here and it may be that it will be necessary to limit these rights to some an extent under

Article 23(1)(i). This reconciliation between *ex post* rights and freedom of expression is the particular focus of the next section of the Guidelines and will considered further below

3. Exceptions from *Ex Post* Rights vis-à-vis Search Engines:

The Guidelines are right to specifically focus on the need to reconcile these *ex post* rights with freedom of expression including its sub-right, the freedom of information. However, it currently places too much focus on the specific exceptions to the right to erasure set out in Article 17(3). Rather than looking at any specific subjective rights of data subjects to secure compliance, the logical starting point is to delimit the substantive duties of controllers and to ensure that these are consistent with fundamental freedoms. Secondly, as the commentary in the draft Guidelines itself demonstrates, most of the specific restrictions listed in Article 17(3) are not really relevant. Indeed, it is really only the exemption from the right to erasure where processing is *"necessary for exercising the right to freedom of expression and information"* (GDPR, art. 17(3)(a)) that can have any real bite here. Thirdly, and again as the draft Guidelines themselves acknowledge at least in relation to the right to object, other subjective rights may be independently invoked in order to secure *ex post* action on the part of a search engine. These other rights must also be reconciled with freedom of expression.

Turning to consider the fundamental duties placed on controllers, these obligations including in particular the data protection principles (GDPR, art. 5) and the legal grounds for processing (GDPR, art. 6) must always be interpreted consistently with freedom of expression as far as this is possible. In some cases, the processing of specific data by search engines might be considered to be *prima facie* inconsistent with these provisions and yet stopping all processing would disproportionately impact freedom of expression. A clear example is contained in *GC et. al. v CNIL* where was recognised that the ongoing dissemination of out-of-date information concerning an individual's legal proceedings might *prima facie* data protection principles related especially to the relevance standard.[13] However, the initial reaction to this should be to consider whether some lesser form of action might result in processing which (having regard to the importance of freedom of expression) can itself be seen as reflective of the underlying legal duty. Indeed, it is in this context that the Court in *GC et. al. v CNIL* mandated that a search engine must after requisite notice ensure that its overall profiling of the data subject was reflective of their current legal position including, in particular, placing a link containing up-to-date information first in any returned listed.[14] Indeed, even more so that in the Directive, there is a strong presumption that both the data protection principles and the legal grounds for processing should not be entirely disapplied (outside of the journalistic and other special expressive purposes (GDPR, art. 85(2)) which are not applicable here).[15]

Nevertheless, it must be recognised that data protection duties (and potentially also some of the data subject rights like the right to rectification and to restriction) may set out peremptory obligations which are simply inconsistent with freedom of expression. Again, the *GC et. al. v CNIL* case explored an example in the default restrictions on the processing of special category and criminal-related data which are set out in Article 9(1) and 10 of the GDPR. In these contexts, and notwithstanding the data subject can point to a *prima facie* violation, a derogation *must* be provided for. Relevant derogatory standards are laid down in Article 9(1)(g) as regards the lifting of the prohibition of processing special category data, Article 10 as regards the lifting of restrictions on processing of criminal-related data and otherwise in Article 23(1)(i) (the *"rights and freedoms of others"* clause). In *GC et. al. v CNIL* the Court indicated that the derogations in Article 9(1)(g) and Article 10 should be treated as self-executing in the absence of implementing Union or Member State legislation. However, since it was also noted that the exercise of any derogation must be *"in compliance with the conditions laid down in those provisions"*, it is clear that both the Union and Member States remain competent to (and indeed should) enact such rights-complaint specifying legislation. Finally, in the absence of this, any use of the derogation must only be as *"strictly necessary"*.[16] This construction makes sense of an admittedly complex and imperfect legal situation. It should therefore also be extended and applied to derogations more generally using the general restriction standards laid down in Article 23(1)(i).

As previously emphasised, subjective data subject rights should be interpreted consistently both with freedom of expression and with these core data protection duties. Thus, as regards to the right to object, it follows that the controller should be able to justify ongoing processing where there is a *"compelling"* (GDPR, art. 21(1)) case under freedom of expression for continuing to ensure access to the information through the relevant processing at issue (e.g. a name-based or image-based search). Meanwhile as regards the right to

[13] *GC et. al. v CNIL* at [74]-[75].

[14] Ibid at [78].

[15] Thus, both are in principle excluded from being restricted under Article 23(1)(i). Moreover, especially given that a whole range of other provisions within chapters II and the III of the GDPR are included in this restrictions clause, that can hardly be considered a legislative oversight.

[16] *GC et. al. v CNIL* at [68].

erasure and where a *prima facie* breach of duty has been established, the exemption for the necessary exercise of the right to freedom of expression and information (GDPR, art. 17(3)(a)) should be interpreted in line with the derogatory scheme above. Thus, where the *prima facie* breach relates to the data protection principles (GDPR, art. 5) or the legal grounds for processing (GDPR, art. 6) then all reasonable steps should be taken to ensure that, interpreted with regard for freedom of expression, the processing as a whole complies with these provisions. In other cases, the derogatory tests set out elsewhere in the instrument should be applied (directly if necessary), namely, Article 9(1)(j) (where the prima facie breach relates to processing special category data without a clear and *sui generis* legal ground), Article 10 (article 9(1)(j) (where the prima facie breach relates to processing criminal-related data without a clear and *sui generis* legal ground) and Article 23(1)(i) (in all other cases). Whilst the detail of the mandatory requirements of derogation differ somewhat under these articles and Article 10 concerning the criminal-related data restriction is particularly unique, these tests (alongside the contextual interpretation of Articles 5 and 6) can provide a structured framework for ensuring that the essence of data protection is respected alongside the provision of necessary and proportionate safeguards for freedom of expression and information.

Dr David Erdos
4 February 2020