ACCESS NOW POSITION PAPER: UNDERSTANDING THE "RIGHT TO BE FORGOTTEN" GLOBALLY

accessnow

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world. By combining innovative policy, global advocacy, and direct technical support, we fight for open and secure communications for all.

TABLE OF CONTENTS

INTRODUCTION

Since 2014, the so-called "right to be forgotten" has been a significant focus of the global debate on privacy and free expression. The debate has its roots in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, known as the Google Spain ruling. In the ruling, the EU Court of Justice detailed the protection arising from the existing right to erasure. Specifically, the court established that users can ask search engines to delist certain URLs from search results when searches are conducted using their name, if the content on the web pages in the results includes information that is "inadequate, irrelevant or no longer relevant, or excessive."

While the decision was aimed at protecting users' privacy, it is a source of deep concern for free expression advocates because of its risks for misinterpretation and abuse. These risks have materialised in countries that may have intended to replicate the European decision, but either misinterpreted the ruling or failed to provide adequate safeguards for free expression rights.

This brief outlines the two components of the "right to be forgotten": the "right to erasure" and the "right to de-list." For reasons explained below, Access Now finds the latter problematic and cannot support it — although we do offer safeguards to mitigate risks given that de-listing practices are taking place globally. In addition, this brief provides:

→ **Recommendations for governments considering their own implementation of the right to de-list,**

→ **a closer look at how the right to de-list is now being implemented in regions across the globe.**

I. "RIGHT TO BE FORGOTTEN": RIGHT TO ERASURE & RIGHT TO DE-LIST

The "right to be forgotten" emerges from European data protection law and includes two different aspects: first, what was traditionally referred to as the "right to erasure," and then, following from the Google Spain ruling, the "right to de-list" or the right to obscurity.

The **right to erasure** allows individuals to delete all personal data related to them when they leave a service or application. This right to erasure is essential to ensure user control over personal information.

The **right to de-list** allows users to request that search engines remove web addresses from results when a search is done using their names.

While Access Now supports the right to erasure, we **cannot support establishing a right to de-list or a right to obscurity**. If it is misinterpreted or implemented the wrong way — particularly in the absence of a comprehensive data protection law and with inadequate transparency — it poses a significant threat to human rights. **It must under no circumstances be misinterpreted or misapplied to enable the removal of online content, including from news media or social media**.

Even in the midst of continued debate, courts and legislators around the world have demonstrated significant interest in developing measures to establish a right to de-list. To help mitigate the risks of abuse and harm to human rights, we have identified a series of legal safeguards that a country must put in place if it is to develop and implement such a right.

II.
SAFEGUARDS FOR IMPLEMENTING A RIGHT TO DE-LIST

While we cannot support the right to de-list or the right to obscurity, as noted above these practices are underway globally. Therefore we believe that countries seeking to enact a right to de-list should provide clear safeguards for its implementation:

1

A right to de-list must be limited to the sole purpose of protecting personal data

Legislators should advance measures to establish a right to de-list solely as a data protection measure. Under no circumstances should such a right be established in the context of defamation legislation or legislation protecting honour.

Further, the right to de-list must be embedded within a comprehensive data protection framework. If no comprehensive data protection law exists, establishing a right to de-list should be put on hold.

2

Criteria for de-listing must be clearly defined in comprehensive data protection legislation to avoid interference with human rights

Lawmakers must clearly define the criteria that govern de-listing requests in comprehensive data protection legislation. The ability to de-list must not interfere with human rights, including the right to freedom of expression and access to information.

Under no circumstances should a right to de-list lead to the deletion of online content. Web addresses may be de-listed in specific search results, but the content must remain online. The specific de-listed URL must also remain in the search engine index, so it can be found when users conduct a search that does not include the name of the individual who requested the de-listing.

3

Competent judicial authorities should interpret standards for determining what is de-listed

It is for the courts to interpret and clarify the de-listing criteria set by the law, and to evaluate its application, if necessary.

Private actors should not be required, nor should they be authorised, to determine the validity of a de-listing request, and they should not be put in a situation where they have a de facto judicial role over content. If legislation is not clear regarding liability, companies may perform excessive de-listing of content, risking unnecessary, disproportionate limitation of free expression outside the rule of law. Instead, search engines should follow clear assessments from, or direct orders by, competent judicial authorities.

4

The right to de-list must be limited in scope and application

Implementation of a right to de-list should be limited to a "data controller" — an entity that determines which personal data is being processed and for what purposes — such as a search engine. It should not be extended to services such as social media platforms where individual users have control over the information displayed.

To avoid search engines taking action outside the rule of law, lawmakers must carefully consider the geographical application of a right to de-list. An absolute interpretation, where the right is limited either to one jurisdiction, or applies to all jurisdictions, raises challenges. The internet is global in nature and widespread use of tools such as Virtual Private Networks could mean that de-listed content will remain accessible in a country where it is meant to be obscured. Moreover, the information that users wish to de-list in searches using their names might have cross-border or local implications that argue against de-listing. It is therefore necessary to develop case-by-case assessment to evaluate which approach provides the highest level of protection to users' rights in each case.

The right to de-list gives individuals the ability to exercise control over their personal data by empowering them to make specific information about them harder to find. However, this process also creates risks to the right to access information. To limit these risks, the right to de-list should be available only to individuals who are not public figures such as celebrities or politicians. In addition, information that is relevant to the public interest should not be de-listed, regardless of the identity of the individual making the request.

Finally, information made available by public authorities, including through public records, should be excluded from the scope of the right to de-list, without prejudice to the data protection law authorising the withdrawal of consent for the publication of personal data. This exclusion is necessary to safeguard transparency, accountability, and the right to access information. The right to freedom of information is an absolute limit to the right to de-list.

5

Search engines must be transparent about when and how they comply with de-listing requests

Search engines implementing de-listing requests must be transparent about their internal compliance process. Companies that offer search engine services should publish transparency reports regularly, illustrating how they comply with the right to de-list through policy and practice by providing aggregate statistics on requests and how often they are rejected, among other data.

If a comprehensive data protection law is in place, and a court order based on the law is issued that requires search engines to assess de-listing requests, companies must be transparent about how they make such evaluations and what safeguards are in place to ensure that individuals' rights to privacy and free expression are respected.

6

Users must have easy access to remedy

Whether the search engine has accepted or rejected a de-listing request, users should have easy access to remedy and a process to challenge the decision at either their local data protection authority or in court.

It is important to note that remedy is only possible if the search engines are not tasked with assessing de-listing requests. Otherwise, the assessment would become an internal commercial decision which, logically, cannot be legally challenged — as a search engine cannot be forced to re-list content. Under no circumstances should laws and corporate policies limit the user's right to seek judicial remedy regarding a de-listing request.

III.
THE RIGHT TO DE-LIST AROUND THE WORLD: CASE STUDIES

Note: These cases studies are not meant to be comprehensive, but instead representative of how the right to de-list is implemented in countries or regions around the world. As the legislative and legal situation evolves, we may revise and update these case studies and/or add new ones.

THE EUROPEAN UNION

The EU has had the right to erasure — distinct from the right to de-list — enshrined into law since 1995 through its Data Protection Directive. The law established that individuals in the European Union could ask for their personal data to be erased once that data is no longer necessary. This right makes it so that if an individual makes a request, providers such as Facebook, Spotify, or Gmail must delete all the data they hold pertaining to the individual once the user leaves the service. This right has been retained in the newly adopted General Data Protection Regulation (GDPR), under the article on the "right to be forgotten".

In the 2014 Google Spain case, the EU Court of Justice ruled that if an individual makes a request, Google and other search engines must de-list certain web addresses from search results when a search is conducted using the name of the person making the de-listing request. However, this ruling did not require search engines to remove de-listed links from the search index. They must remain accessible when users conduct searches using terms other than the name of the individual making the de-listing request.

The court has developed a set of criteria for search engines to consider when they receive a de-listing request. Search engines must grant a de-listing request only if the personal information included in the designated web address is "inadequate, irrelevant or no longer relevant, or excessive", and only if the information does not pertain to a public figure or is not of public interest.

However, more guidance is necessary to ensure that search engines do not to over- or under- reach compliance with the ruling. There are efforts afoot to develop guidelines to help search engines assess de-listing requests and determine whether a request involves a public figure or implicates the public interest, initiated by the Article 29 Working Party (comprised of representatives of the data protection authorities of the EU member states, the EU Data Protection Supervisor, and the European Commission). These efforts ought to be furthered at EU level. The government should also develop broad discussion on the issue of intermediary liability. Even though the General Data Protection Regulation, specifically aimed at upgrading and strengthening users' privacy rights, is not the right vehicle for addressing this issue, it remains urgent for the EU to develop legislation to protect free expression and set clear rules for the role and the liability of intermediaries.

Until such rules are established, however, the EU Court of Justice should provide further guidance to assist search engines in the case-by-case assessment of de-listing requests. For their part, search engines should be more transparent about the criteria they have been using to assess these requests.

Regarding scope, the court has not provided clarity regarding geographical application of the right to de-list, but has made clear that individuals can request de-listing only from a "data controller" — an entity that determines which personal data is being processed and for what purposes. The court ruled that search engines fit that definition (since, for example, they use algorithms to determine how search results are listed and placed). However, individuals cannot request de-listing of information published on social media platforms like Facebook or Twitter, because under EU jurisprudence private posts or tweets fall under the so-called household exception. In that case, the user that publishes content or information on social media is the "data controller."

Finally, in the current implementation of the right to de-list in the EU, access to remedy is limited. The only form of recourse that a user has is the opportunity to challenge a search engine's decision to deny a request to de-list. There should be more clarity on venues for remedy, and this protection should be extended.

Evaluation and recommendations for the EU

What is in place

1. Data protection law. The recently adopted GDPR brings a strengthened enforcement mechanism.
2. The right to de-list is based on a data protection law.
3. The EU Court of Justice has developed criteria for its application.
4. A right to de-list request does not constitute a request for removal of content.
5. The right currently does not apply to social media platforms.

What needs work

1. More guidance is needed from Article 29 Working Party to help search engines assess de-listing requests.
2. More clarity is necessary to govern the geographical application of the right to de-list.
3. Individuals need better access to remedy whether a request to de-list is approved and denied.

LATIN AMERICA

Latin American countries have diverse levels of data protection under a variety of legal frameworks, as well as a number of different strategies for regulating it. According to the DLA Piper's Data Protection Laws of the World Handbook, most countries in Latin America have a moderate level of protection, including Mexico, Costa Rica, Colombia, Peru, Chile, and Uruguay. Countries like Honduras, Venezuela, and Brazil are considered to have limited frameworks. Some countries, like Brazil, are currently discussing adopting a general data protection act, while others, like Argentina and Chile, are contemplating reforming their data protection frameworks. Based on the same ranking, Argentina is considered the Latin American country with the most robust data protection in place. Argentina is also currently one of only two countries in Latin America that the European Commission recognises as having an adequate level of data protection. The other is Uruguay.

When creating national legislation on data protection, several countries in Latin America have mirrored EU's Data Protection Directive, which encompasses the right to erasure. In the aftermath of the Google Spain ruling, lawmakers in the region have launched discussion on the "right to be forgotten", notably in Brazil, Argentina, Colombia, and Chile. However, discussion in these jurisdictions has involved different interpretations of the right to de-list, implicating varying levels of risk to human rights.

ARGENTINA

In Argentina, for instance, lawmakers are proposing bills that address the issue not from a data protection perspective, but through expansion of the concept of defamation. This approach is dangerous, threatening significant damage to the internationally protected human right to freedom of expression by stripping away the necessary public interest considerations. As we explain above, the Court of Justice of the EU clearly stated that matters of public interest — including information about public figures — must be excluded from the right to de-list.

BRAZIL

Brazil is also a case of deep concern. Despite having sectorial legislation on the subject, it does not have a comprehensive data protection framework in place. At the same time, Brazil has a history of abuse of the right to free expression and access to information. It has been criticised internationally for its extended use of defamation lawsuits to silence political opposition and critics of public authorities. Legal and human rights experts have, for example, denounced Brazil's criminalisation of so-called honour crimes before international human rights' bodies.

Human rights organisations are raising the alarm, pointing out that if the right to de-list is implemented in Brazil, or implemented in an ill-conceived way, it will serve as an instrument for abuse and violations of the right to free expression. Worryingly, while lawmakers in Brazil have been eager to advance bills focusing on a right to de-list — with at least three bills under discussion — they have paid scant attention to approving the necessary precursor to establishing that right: a comprehensive data protection act that properly frames the right solely as a data protection measure.

COLOMBIA

Colombia has a different approach to the right to de-list, stemming from a ruling by the Colombian Constitutional Court in 2015, which granted the plaintiff's request to apply a right to de-list to a newspaper article published online that described the plaintiff's alleged involvement in criminal activities.

The court found that an individual has the right to ask that specific links to web pages that have outdated information about the individual be made inaccessible. However, in contrast to the Google Spain ruling in the EU, the court imposed the obligation to de-list the pages from search engines on the original publisher — in this case, the newspaper — rather than the search engines themselves. The newspaper was ordered to use technical measures, such as the robots.txt file, to ensure that the pages would not be listed by search engines. Further, the court ordered the newspaper to prepare an update clarifying the situation regarding the plaintiff with respect to the criminal accusations under dispute.

Notably, in Colombia, the search engine is relieved from the obligation to de-list the page or even dealing with the issue. The only "data controller" of interest is the newspaper; the search engine is considered a mere intermediary deserving protection on freedom of expression grounds.

Evaluation and recommendations for Latin America

What is in place

1. Several countries in Latin America have data protection rules in place. However, the frameworks are often limited or outdated.

What needs work

1. Countries that do not have a comprehensive data protection framework should develop one, and advance their courts' interpretation of data protection principles and mechanisms, before contemplating establishing a right to de-list.
2. Countries must not establish a separate right to de-list outside of a data protection framework, and not in the context of defamation law or honour protection. This is a particular threat in countries where public authorities have a history of abusing the rights to freedom of expression and access to information.
3. If the right to erasure is established, it must be properly implemented to protect citizens against the unauthorised treatment of their personal data by internet companies or other data processors.

Evaluation and recommendations for Latin America

4. Any right to de-list must exclude from the scope of application public figures and information of public interest.
5. Under no circumstances can a right to de-list request lead to removal of online content, even when a publisher is required to exclude the content from search engine indexing.
6. If a right to de-list is established, it's necessary to provide clarity on the scope of application.
7. If a right to de-list is recognised, there must be remedy mechanisms in place for users.

RUSSIA

In January 2016, Russia's transposition of the law on the "right to be forgotten" entered in force. While the law was introduced in the aftermath of the Google Spain case, its provisions differ greatly from the rights established under EU data protection law and the recommendations made by the EU Court of Justice. These divergences makes it a threat to human rights.

The law gives Russian citizens the right to request search engines to remove links about them that are in violation of Russian law, inaccurate, out of date, or irrelevant because of subsequent events or actions taken by the citizens. Due to its failure to provide safeguards to protect the right to freedom of expression and access to information, the law has a chilling effect on expression, and will likely lead to censorship. The law requires the removal of content from a search engine index — rather than de-listing — and it does not exclude information related to a public figure or of the public interest.

Evaluation and recommendations for Russia

What is in place

1. While Russia currently has data protection measures in place at the federal level, as well as specific sectoral rules, its implementation and the development of data localisation measures through these laws raises concerns for the protection of fundamental rights and often appear to contradict the purpose of the legislation.

What needs work

1. Russia must develop safeguards to protect privacy and free expression.
2. Russia should amend the law so that a right to de-list request does not lead to removal of online content.
3. The country must exclude from the scope of application public figures and information of public interest.
4. A remedy mechanism must be put in place.
5. The country should clarify the basis of this right, and the scope of its application.

HONG KONG

In 2015, the debate on the right to de-list reached Hong Kong through an appeal launched by David Webb, a website owner, against an enforcement notice under the Hong Kong Data Protection Ordinance.

Webb's website has an online database containing information about the roles certain individuals play in the financial and public sectors in Hong Kong. The database also includes reports and links to public documents about these individuals, such as press articles and court judgments. For example, it provides access to details such as the full names of the parties in the court judgment of a matrimonial case that was heard in open court in Hong Kong. The judgment was made publicly available in 2002, but in 2012, was redacted by the court. The Hong Kong privacy commissioner therefore ordered Webb to remove the names from his online database.

Webb decided to appeal, claiming that the data had been available in the public domain. Webb lost the case, with the court confirming that he had infringed the "data usage principle" of the Hong Kong Data Protection Ordinance.

This case involves the intersection of the right to privacy, freedom of expression, and the right to use personal data in the public domain. Notably, it was resolved under the framework of key data protection principles: data usage and users' consent. That is, while the issues intersect with those in other right to de-list cases, the Hong Kong case does not involve de-listing. It has nevertheless sparked debate about establishing a "right to be forgotten" in Hong Kong, and the country may well consider legislation in this area.

Evaluation and recommendations for Hong Kong

What is in place

1. Data protection law, with efficient enforcement.

What needs work

2. If a right to de-list is established, the Data Protection Ordinance should be amended to set clear criteria for its scope and application, and put human rights safeguards and a remedy mechanism in place.

INDIA

In India, the right to de-list is currently under discussion in the context of two lawsuits filed by individuals requesting that personal information be "removed" from search engines. These individuals would like to assert a right developed in the EU to protect their privacy and prevent discrimination. However, India does not have a separate codified legal instrument to protect privacy or ensure data protection. Courts in India are therefore assessing whether the Indian Constitution's guarantee of the fundamental right to life and liberty encompasses a right to de-list.

It is encouraging that users in India are seeking greater protection for their right to privacy, and its existence and scope is the subject of an upcoming constitutional bench hearing before India's supreme court. However, as several legal proceedings make clear, India is in urgent need of adopting comprehensive data protection legislation, which must be in place before establishing a right to de-list. As we have explained, such a right must be part of a robust framework to protect users' privacy, upholding basic data protection principles such as consent, data minimisation, purpose limitation, a right to access, a right to object, and much more.

Evaluation and recommendations for India

What is in place

1. Constitutional protection for the right to life and liberty, previously held to include an implicit right to privacy.

What needs work

1. India must develop a comprehensive data protection framework before considering putting in place a right to de-list.

SOUTH KOREA

South Korea was one of the first countries to debate the "right to be forgotten" in the aftermath of the Google Spain ruling in the EU. The debate rose to public consciousness when a rapper going by the name MC Mong made an attempt to gain exemption from military service. People were able to find his remarks in an online Q&A platform, where in 2005 the singer publicly questioned whether he could be exempt from military service if he lost a certain number of teeth. The website does not allow users to remove questions once they receive answers. Following intense public debate and consultation regarding the right to de-list, the Korea Communications Commission (KCC), a government agency, pushed the discussion further by developing guidelines aimed at protecting this right.

The KCC's guidelines vary significantly from the right to de-list developed in the EU. First, the principles are not established in law. Second, they primarily concern online users' own posts rather than articles posted by a third party, since Korean law already grants people the right to request the deletion of information by a third party if it is deemed damaging to one's reputation. The guidelines also seek to expand the right to de-list beyond search engines, ordering internet companies to accept removal requests in some "exceptional cases" where a user's control of content was formerly limited or blocked. Last but not least, reports on the guidelines suggest that if a user requests de-listing, the content in question will be deleted. This approach is at odds with the right to de-list developed in the EU, raising serious concerns for free expression and creating risks for censorship.

Evaluation and recommendations for South Korea

What is in place

1. Data protection law.

What needs work

1. If a right to de-list is developed, guidelines and criteria for its application would need to be established in the data protection law with clear safeguards, not developed by a media regulation agency that may not have the competency to protect users' privacy.
2. Remedy mechanisms must be put in place.

CONCLUSION

The Google Spain ruling has led to one of the most engaged discussions on the interaction between the right to privacy and free expression worldwide, two fundamental rights that are mutually reinforcing. However, a misinterpretation of the right to de-list, such as an implementation outside a comprehensive data protection law and with inadequate transparency, poses a significant threat to human rights, in particular the right to receive and impart information.

We encourage legislators around the world with a significant interest in establishing a right to de-list to take the utmost account of the safeguards developed in this paper. If a right to de-list is to be developed, its sole purpose must be to enhance users' control over their personal information. Under no circumstances must the right to de-list be misinterpreted or misapplied to enable the removal of online content.

For more information, please contact:

Raman Jit Singh Chima
Global Policy Director
raman@accessnow.org

Access Now (accessnow.org) defends and extends the digital rights of users at risk around the world. By combining innovative policy, global advocacy, and direct technical support, we fight for open and secure communications for all.