ARTICLE 19

The "Right to be Forgotten": Remembering Freedom of Expression

2016

Policy Brief

ARTICLE 19
Free Word Centre
60 Farringdon Road
London
EC1R 3GA
United Kingdom
T: +44 20 7324 2500
F: +44 20 7490 0566
E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org

ISBN: 978-1-910793-33-6

Executive Summary

In this policy brief, ARTICLE 19 provides comprehensive recommendations on how to ensure protection of the right to freedom of expression with regard to the so-called "right to be forgotten."

The "right to be forgotten" usually refers to a remedy which in some circumstances enables individuals to demand from search engines the de-listing of information about them which appears following a search for their name. It can also refer to demands to websites' hosts to erase certain information. More broadly, it has been considered as a right of individuals "to determine for themselves when, how, and to what extent information about them is communicated to others"[1] or as a right that gives the individual increased control over information about them. It has been categorised as a privacy right even though it applies to information that is, at least to some degree, public.

The "right to be forgotten" is expressly recognised neither in international human rights instruments nor in national constitutions. Its scope remains largely undefined: it ranges from a more limited right protected by existing data protection law to broader notions encompassing the protection of reputation, honour and dignity. It came to the fore with the decision of the Court of Justice of the European Union (CJEU) in the Google Spain case of 2014. In this case, the CJEU held that data protection principles applied to the publication of search results by search engines and that individuals had a right to request that search engines operating in the EU de-list search results obtained by a search for their name. However, this issue is not limited to Europe, as since the CJEU judgement, several states outside of Europe either have adopted a dedicated "right to be forgotten" law or have been looking to adopt new laws on the subject.

ARTICLE 19 is concerned by these developments and the implications of the "right to be forgotten" for the right to freedom of expression. Hence, in this policy brief, ARTICLE 19 proposes a framework solution to the issues raised by the "right to be forgotten," grounded in international human rights law. ARTICLE 19 does not advocate for the recognition of the "right to be forgotten" in domestic or international standards. Instead, this policy brief offers detailed recommendations on how to strike a proper balance between the right to freedom of expression and other rights in this context, and what substantive and procedural safeguards should be put in place in order to protect the right to freedom of expression, if such a "right" is recognised and granted.

Key Recommendations

1. Existing remedies should be pursued such as those offered by privacy and defamation laws, and remedies under the terms and conditions of intermediaries, instead of recognising the "right to be forgotten,";

2. Any "right to be forgotten" should be strictly limited, as certain minimum requirements must be met for such a right to be compatible with the right to freedom of expression, both in terms of substance and procedure. Specifically, the "right to be forgotten" should be limited to private individuals and should be actionable only against search engines (as data controllers), rather than actionable against hosting services or content providers. Any protections should also make explicit reference to the right to freedom of expression as a fundamental right with which such protections must be balanced. Further, decisions on "right to be forgotten" requests should only be issued by courts or independent adjudicatory bodies;

3. A strict seven-part test for balancing the right to freedom of expression and the "right to be forgotten" should be applied, taking into consideration:
- Whether the information in question is of a private nature;
- Whether the applicant had a reasonable expectation of privacy, including the consideration of issues such as prior conduct, consent to publication or prior existence of the information in the public domain;
- Whether the information at issue is in the public interest;
- Whether the information at issue pertains to a public figure;
- Whether the information is part of the public record;
- Whether the applicant has demonstrated substantial harm;
- How recent the information is and whether it retains public interest value;

4. Minimum procedural requirements should be observed, including
- Only courts or independent adjudicatory bodies should decide whether "right to be forgotten" requests should be upheld;
- Data publishers should be notified of "right to be forgotten" requests and should be able to challenge these requests;
- De-listings should be limited in scope, including geographically;
- Relevant service providers, public authorities and the courts should all publish transparency reports on "right to be forgotten."

Table of contents

Introduction

In the digital era, information on the Internet is ubiquitous and seemingly permanently available. The way in which people remember and recall information has also changed significantly, now that much of the world's knowledge is available at the click of a mouse. Search engines have become basic necessities, without which information would be nigh on impossible to find and social media platforms play a crucial role in enabling people around the world to communicate with each other.

The apparent permanence and instant availability of information online has also come at a price. Search engines and social media platforms simultaneously allow access to information that individuals may wish to keep "private" or secret, such as news articles about past crimes, embarrassing old photos, or sex videos posted by ex-partners. Various types of information – be it truthful, false, outdated or taken out of context - may cause harm to individuals, and may threaten important values, such as dignity or personal autonomy, which are protected by the right to privacy under international human rights law. Meanwhile, private companies collect and retain vast amounts of data such as online shopping habits, cultural preferences, political views, and lists of visited websites. All of these developments have led to concerns about misuse and abuse of personal information for unlawful purposes or identity theft. It is not surprising, therefore, that individuals are increasingly seeking to reassert control over their identity and personal information online.

The "right to be forgotten" has been presented as a remedy to this state of affairs. However, this simplified and misleading term is expressly recognised neither in international human rights instruments nor in national constitutions. Nor is it currently explicitly recognised in the vast majority of countries around the world. The scope of this "right" remains largely undefined: it ranges from a more limited right protected by existing data protection law to broader notions encompassing the protection of reputation, honour, and dignity.

In ARTICLE 19's experience, the "right to be forgotten" usually refers to a remedy which would in some circumstances enable individuals to demand from search engines the de-listing of certain kind of information about them which is discovered by a search for their name. It can also refer to demands to websites' host to erase certain information. More broadly, it has been considered as a right of individuals "to determine for themselves when, how, and to what extent information about them is communicated to others"[2] or as a right that gives the individual increased control over information about them. It has been categorized as a privacy right even though it applies to information that is, at least to some degree, public.

The idea of a "right to be forgotten" is not new, however. For example, national law in several countries recognises that, after a period of time, criminal records should be expunged in order to enable the rehabilitation of offenders in society. Further, it is a familiar concept in newsrooms, where news is a perishable commodity, that information loses relevance over time.

At the same time, the more problematic aspects of a "right to be forgotten" must not be overlooked. Information that may seem trite or trivial to some may be highly relevant to the work of historians, archivists and libraries. Equally, news archives have long been the repositories of our collective memory about world events. Court decisions, bankruptcy filings and other public records are often expected to remain accessible for indefinite periods of time. Consequently, it would be simplistic to suppose that, just because information is about a person and dated, it should therefore be deleted or de-listed from search results. At its core, the "right to be forgotten" involves making certain information about individuals harder to find, even if it is information that has legitimately been in the public domain for decades. As individuals are empowered to hide true but embarrassing information about them, the potential for abuse becomes clear.

The "right to be forgotten" came to the fore with the decision of the Court of Justice of the European Union (CJEU) in the Google Spain case of 2014. In that case, the CJEU held for the first time that data protection principles applied to the publication of search results by search engines. The CJEU held that individuals had a right to request that search engines operating in the EU de-list search results obtained by a search for their name. As domestic courts, data protection regulators, search engines, and experts on privacy and freedom of expression have scrambled to come to grips with the implications of the "right to be forgotten," several governments around the world have followed suit, either adopting a dedicated "right to be forgotten" law[3] or looking to adopt new legislation on the subject.[4] The "right to be forgotten" is therefore no longer a uniquely European idea but instead has taken on a broader significance. There is also a serious risk that the limited safeguards for the right to freedom of expression that were recognised by the CJEU might be missed or ignored by governments who have a poor record on freedom of expression or who want to undermine the free flow of information.

It is vital that the right to freedom of expression is remembered in the debate. ARTICLE 19 does not advocate for the recognition of the "right to be forgotten" in domestic or international standards. Our focus is pragmatic, and we intend to foster more informed debates about the implications of "right to be forgotten" for freedom of expression and human rights in general. In this policy brief, we therefore propose a framework solution to the issues raised by the "right to be forgotten," grounded in international human rights law and our extensive experience in balancing these rights. Ultimately, the issue at hand is how to strike a proper balance between the right to freedom of expression and other rights in this context. Hence, the policy brief makes detailed recommendations as to the proper substantive and procedural safeguards that should be put in place in order to protect the right to freedom of expression.

International human rights standards

Right to freedom of expression and information

The right to freedom of expression and information (freedom of expression) protects the free flow of information, opinion and ideas. It applies to all media and regardless of borders. It includes the right not only to impart but also to seek and receive information. Freedom of expression has long been recognised as fundamental to both individual autonomy and a free society in general.[5]

The right to freedom of expression is recognised in nearly every national constitution and in most international human rights treaties including the Universal Declaration of Human Rights (UDHR),[6] the International Covenant on Civil and Political Rights (ICCPR),[7] the African Charter on Human and Peoples' Rights (African Charter),[8] the American Declaration of the Rights and Duties of Man (American Declaration),[9] and the American Convention on Human Rights (American Convention),[10] and the European Convention on Human Rights (European Convention).[11]

In General Comment No. 34, the UN Human Rights Committee (HR Committee) - the treaty body that authoritatively interprets the scope of states' obligations under the ICCPR - re-affirmed that freedom of expression is essential for the enjoyment of other human rights and confirmed that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all electronic and Internet-based modes of expression.[12] In other words, freedom of expression is protected online in the same way as it is protected offline.

However, Freedom of expression is not absolute. International standards make it clear that freedom of expression is a qualified right which may be limited, provided the restriction complies with a three-part test. The restriction must:

- be provided by law;
- pursue the legitimate aims explicitly enumerated in Article 19 of the ICCPR; and
- be necessary in a democratic society. In particular, the requirement of necessity entails that the measure adopted must be proportionate to the aim pursued. If a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure must be applied.

International law thus allows that freedom of expression may be subject to certain restrictions for the sake of other legitimate interests including, among other things, the rights of others. As we shall see in the following section, this includes, in principle, the right to privacy.

The right to privacy

Privacy is a broad concept relating to the protection of individual autonomy and the relationship between an individual and society, including government, companies, and private individuals. It encompasses a wide range of rights including protections from intrusions into family and home life, control of sexual and reproductive rights, and communications secrecy. [13] It is commonly recognised as a core right that underpins human dignity and other values such as freedom of expression and freedom of association.[14]

The right to privacy is recognised in most international human rights treaties[15] and in nearly every national constitution.[16] It has been adjudicated upon by both international and regional bodies.[157] The right to privacy is also legally protected at the national level through provisions in civil and/or criminal codes.[18] Within the Americas, many nations have formalized privacy rights, either in constitutions or laws, under Habeas Data, which gives individuals the right, in the words of the Inter-American Commission on Human Rights, to "modify, remove, or correct ... information due to its sensitive, erroneous, biased, or discriminatory nature."

The right to privacy is not an absolute right and is subject to the same three-part test, namely legality, necessity and proportionality.[19]

Relationship between the right to freedom of expression and the right to privacy

The relationship between the right to freedom of expression and the right to privacy is a complex one. On the one hand, the protection of the right to privacy in online communications is essential to ensure that individuals have the confidence to freely exercise their right to freedom of expression (by retaining their anonymity, for example).[20] However, the publication of private information constitutes a clear infringement of the right to privacy.

At the same time, both rights can be limited under certain circumstances, subject to the three-part test outlined above. This means inter alia that States are not required to adopt measures that would protect the right to privacy where that would constitute an undue restriction on freedom of expression.[21] Simultaneously, under international human rights law, States are obliged to provide remedies for violations of either right.

In other words, freedom of expression and the right to privacy are mutually reinforcing but occasionally conflicting rights. These conflicts can be especially difficult to manage when the information at issue is both personal and public.[22]

Data protection

The right to privacy has evolved to address issues relating to the collection, use, and dissemination of personal information held by governments and private bodies in information systems. [23] Starting in the 1960s, principles governing the collection and handling of this information known as "fair information practices" were developed and adopted by international bodies and national governments.[24]

The principles generally are as follows:

- **Collection Limitation Principle.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- **Data Quality Principle.** Collected personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

- **Purpose Specification Principle**. The purposes for which personal data are collected should be specified in advance or at the time of data collection, and the subsequent use should be limited to the fulfilment of those purposes, or such others as are not incompatible with those purposes, and as are specified on each occasion of a change of purpose.
- Use Limitation Principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified above except: a) with the consent of the data subject; or b) by the authority of law.

- **Security Safeguards Principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure.

- **Openness Principle.** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available to establish the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

- **Individual Participation Principle.** An individual should have the right:
  a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her;
  b) to obtain such data within a reasonable time;
  c) at a charge, if any, that is not excessive;
  d) in a reasonable manner; and
  e) in a form that is readily intelligible to him or her;
  f) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
  g) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

- **Accountability Principle.** A data controller should be accountable for complying with measures which give effect to the principles stated above.

Internationally, the principles have been adopted by the UN General Assembly[25], the Commonwealth[26] and the Economic Community of West African States (ECOWAS).[27] In Europe, both the Council of Europe[28] and the European Union[29] have incorporated these principles into data protection treaties; with the EU Data Protection Directive being the most influential.[30] Similar principles are also under consideration by the Asia-Pacific Economic Cooperation (APEC) forum.[31]

At the same time, the rise of data protection law raises significant issues for the protection of freedom of expression online, particularly in the wake of the CJEU's judgment in the Google Spain v Costeja case.[32] In particular, as later examined in more detail, the CJEU's decision highlighted difficult questions about the interplay between data protection law, defamation law, privacy law and the liability of Internet intermediaries for third-party content.

The "right to be forgotten"

Legal basis

Origins of "the right to be forgotten"

The underlying basis for "the right to be forgotten" lies in the argument that information may lose importance over time and that access to it should therefore be restricted. This has been accepted as part of criminal law and aspects of civil law in a number of respects:

- **Criminal records:** Legislation in a number of countries has recognised that after a given period of time, convictions for certain types of offence are to be regarded as spent, i.e. that convicted individuals are to be treated for all purposes in law as persons who have not committed the offence.[33] These laws seek to ensure the rehabilitation of offenders by enabling them to live their life without undue prejudice based on past mistakes for which they have now repaid their debt to society. In practice, this means that the criminal record of these individuals is expunged or considered as "clean." In some countries, it also means that individuals have a right to request that news media coverage related to their conviction be purged from news archives once the person in question has served the sentence.[34]

- **Statutes of limitations:** The law generally recognises that after a certain period of time, the publication of information that infringes a person's privacy or damages their reputation may no longer be actionable. In common law countries, this is referred to as a limitation period (or sometimes a 'statute of limitations'); in civil law countries, it is called 'prescription.' In the context of defamation and privacy claims, the concept of limitation periods reflects the idea that certain wrongs relating to the publication of information no longer require reparation because any harm caused by the publication has long since been resolved and it is deemed best that society move on.

However, although the law sometimes allows that some information may lose significance over time, it is nonetheless widely accepted that certain types of information must be collected and remain accessible for the preservation of the historical record, to redress past human rights abuses and to fulfil the public's right to know:

- **Archives:** It is generally accepted that libraries, national archives and newspapers, as the repositories of human history and collective memory, collect all sorts of information. They have long maintained archives, which may include personal information about ordinary individuals. While national archives may retain personal data permanently for the purposes of research or history, they generally remain subject to data protection law so that certain categories of information may not be retained, or access to such information may be restricted, if it would cause substantial harm to the data subject.[35] Newspaper archives also benefit from additional exemption under data protection principles with regard to journalistic material.

- Information about past human rights abuses and the "right to truth": Although the "right to truth" is not expressly recognised under international law,[36] several countries have adopted policies that seek to ensure that victims, their families, and society as a whole have access to information about past egregious human rights violations, e.g. the human rights abuses committed during military dictatorships.[37] In this way, the Inter-American Commission on Human Rights has recommended that member states of the Organisation of American States (OAS) should adopt measures to classify, systematise, preserve and make available historical archives about serious violations of human rights and violations of international humanitarian law.[38]

- **"Lustration":** After the fall of the communist regime, several post-communist countries adopted "lustration" legislation which sought to "cleanse" the new regime of government officials or other individuals who had collaborated with the previous regime or been involved in human rights violations.[39] This involved measures ranging from the publication of information about collaboration to the dismissal and bans on holding certain offices, particularly in government or the judiciary.[40] In some countries, the legislation also gave the public a right of access to the files of individuals who performed certain functions (such as collaboration with secret police), although access to sensitive information could be limited.[41]

- **Freedom of information laws:** Freedom of information principles generally recognise that the public have a right of access to information held by public bodies, which may sometimes include personal information. Access to information may be limited subject to certain conditions, including whether disclosure of such information would cause substantial harm to the privacy interests of the individual concerned, and whether there is an overriding public interest in making the information available.[42]

The "right to be forgotten" online

In the online context, several legal bases for the "right to be forgotten" can be identified, in particular:

- **Data protection law:** In a majority of countries, the "right to be forgotten" that may be asserted against search engines has been derived from data protection law.[43] For this reason, in the EU, the key test to be applied in "right to be forgotten" cases is whether the personal information at issue is "inadequate, irrelevant or no longer relevant."[44] At the same time, search results containing personal information may not be de-listed when the retention of these results is in the public interest, for instance because of the data subject's role in public life.[45] Moreover, the information is not removed from the original site and may be accessed directly or by using different search terms.

- **Privacy, personality rights, and defamation law:** The Internet presents new challenges for claimants in privacy, personality rights, and defamation cases. Whereas in the past, these types of cases were primarily remedied by pecuniary damages, they are now also dealt with by way of 'notice-and-takedown' measures, under hosting service providers' Terms of Service or equivalent intermediary liability laws.[46] Some courts have also issued injunctions against website operators to prevent the disclosure or further dissemination of sex tapes in so-called 'revenge porn' cases.[47] These types of cases are sometimes described as "right to be forgotten" cases despite the fact that they concern the removal of information from websites rather than the de-listing of search results by search engines.[48] It is important to bear in mind that the removal of information from websites, (i.e. at source), in principle means that the information is no longer available through any search, whereas the more limited right to be de-listed under EU law only makes information less easy to find using certain search terms. At the same time, it is argued that the "right to be forgotten" is a more effective remedy for individuals in these type of cases than seeking the "takedown" of data:

  - The scope of the information that may be removed on the basis of a privacy or defamation action is generally narrower than that under data protection law;
  - The process of seeking the de-listing of search results by search engines is generally quicker and easier than pursuing privacy claims;
  - It is extremely difficult to achieve full "take down" of information even with a court order after a privacy claim due to the multiplicity of websites that may be involved and jurisdictional issues.

- **The right to remove one's own content:** Another – more limited – iteration of the "right to be forgotten" involves the right for children and young people to remove postings they have created themselves from websites, online and mobile applications.[49] It has also been promoted as a means of protecting children from the negative consequences of juvenile errors.[50] However, it is important to note that such a provision does not include a right to request that material posted by third parties be removed.

Arguments in favour of the "right to be forgotten"

The "right to be forgotten" is seen by many as a positive development for individual self-determination in the digital age. In particular, data protection and privacy advocates point to a number of arguments in support of recognition of the right:

- **Individuals should have a right to control their personal information and identity in the digital age:** Information communication technologies allow both government and private entities to significantly interfere with an individual's right to privacy by enabling them to track and record all activities online. Meanwhile, individuals are encouraged to share a considerable amount of information about themselves on social media in an unprecedented manner. It is therefore the responsibility of governments and lawmakers to protect the right to data protection and privacy lest people lose their ability to manage their identity and personal integrity. Moreover, individuals should have ownership of their personal information. The "right to be forgotten" thus empowers people to regain control over their digital lives.

- **Most personal information available online has no public interest value:** Digital technologies have fostered an era of information overload. Some argue that only information that is relevant and in public interest should have its accessibility safeguarded, and that not all information is of this nature. The vast majority of personal information available online is of limited intrinsic value, whereas its accessibility could have disastrous consequences on people's lives: such information may thwart their employment prospects, hamper their ability to obtain the credit they need, or simply prevent them from living their lives with dignity.

- **There is no right to access information which is unlawfully in the public domain:** Certain personal information in the public domain is there unlawfully, such as intimate photos distributed on the Internet without consent. There is no justification for other people to have access to such information.

- **People should not be indefinitely reminded of their past mistakes:** Even when information is lawfully in the public domain or originally shared by the individual with his or her consent, people have a right to make mistakes without being haunted by them indefinitely. This is already recognised by the law in relation to spent convictions; the same should be true in the digital environment. Failure to recognise the "right to be forgotten" allows a distorted view of individuals to be presented by search engines which list links to juvenile or other errors in top search results for a person's name. In the case of children, this might impede their development and diminish their sense of self-worth. Furthermore, the original publication may have been authorised at a time when their capacity to properly consent or understand its implications was under-developed.

- **It is a form of the "right of reply" in the context of internet searches:** In many countries, the law already recognises a right of reply or right of correction against false information published or aired in print or broadcast media. There is no reason in principle why an equivalent remedy to the right of reply should not exist for search results in order for individuals to contextualise information about themselves. Since it is currently not technologically feasible to enable such a right of reply for search results, the "right to be forgotten" is the next best option.

- **It is compatible with the right to freedom of expression:** In the Costeja decision, the CJEU took freedom of expression concerns into account, including by holding that in certain circumstances, such as when the personal data in question relates to a public figure, the right of the public to have access to that information might prevail. Moreover, the information itself remains available and can be found on the web using search terms other than the name of the individual at issue.

Arguments against the "right to be forgotten"

ARTICLE 19 recognises the concerns of data protection and privacy advocates in the face of the mass collection of our personal data by public and private actors. Further, we agree that it is vital that the right to privacy be protected in the digital age. However, we believe that proponents of a "right to be forgotten" fail to appreciate the following issues:

- **Individuals do not and should not have an unqualified right to control the accessibility of information about them:** Simply because information is about an individual does not mean that that information belongs to them or that they should be able to control it in a proprietary sense. In particular, individuals should not be able to restrict access to information about them which has been published by third parties, except where that information is private or defamatory and its publication is not otherwise justified. In other words, information about individuals may also equally "belong" to the public, who should therefore not be prevented from accessing that information. For example, the fact that a particular individual was declared bankrupt over a decade ago is not simply information about that person. It also involves his/her debtors as well as a declaration in open court. The idea that it is the individual who should retain ultimate control over that information is not only a self-centred approach but also ignores the broader right of the public to share and receive material that is legitimately in the public domain.

- **There is a public interest in freedom of expression:** In general, no justification should be required for the publication of information which is not private. Moreover, what most people would consider to be trivial or irrelevant information may provide cultural insights of great value to historians. Insofar as that information may already be public, there is a strong interest in preserving it and in it remaining easily accessible for research, archiving or due diligence purposes. Data protection authorities themselves consider that the collection of historical and cultural data – which may include personal data - should be encouraged and treated as a valid way to retain data beyond its 'operational utility' date.[51]

- **The publication of information which has been unlawfully obtained may nonetheless be in the public interest:** The Internet has opened up the possibility for a wealth of personal and other sensitive information to be made accessible to the world at large. At the same time, the publication of information obtained unlawfully, e.g. as a result of hacking personal computers or unauthorised access to government files, may well be in the public interest and therefore justified.

- **People should be given an opportunity to forgive:** Allowing individuals to obtain the de-listing of certain links associated with their name gives them an opportunity to present a distorted picture of who they are. Individuals who seek access to information about others should be able to form their opinion of them on the basis of all the information available rather than on the basis of links which have been selected for publication and ranked in such a way as to present someone in a more favourable light. In this sense, individuals should be given an opportunity to forgive or overlook past mistakes rather than for those mistakes to be 'forgotten' at the behest of those who have made them.

- **The "right to be forgotten" is more restrictive of freedom of expression than the right of reply or correction:** The right of reply or the right of correction enables individuals to either present their side of a story or correct factual mistakes without the information in question being made more difficult to locate. On contrary, the "right to be forgotten" allows individuals to remove or render information about them far less accessible and is therefore much more problematic for freedom of expression.

- **Deriving the "right to be forgotten" from data protection law is problematic for several reasons:**
  - Data protection concerns the protection of "personal data" - i.e. data about a person - which may be either private or public. It grants individuals a right to request the de-listing of information about them, simply on the ground that it is "no longer relevant." Media law concepts that protect freedom of expression - such as "reasonable expectation of privacy," "serious harm" or the "public domain" - are not taken into account. Hence, the upshot of the application of data protection law to the publication of search results is that perfectly lawful content may become less accessible simply because individuals want to hide embarrassing information about themselves.
  - The fact that the information at issue remains available is of limited assistance in circumstances where a 'name' search might be the only effective way of finding it. In this sense, making the information harder to find may prevent access to it altogether.
  - Data protection law puts search engines in the position of having to determine whether personal data is 'inadequate, irrelevant or no longer relevant' and subsequently whether it should therefore be de-listed, which is deeply inappropriate. In particular, search engines lack the independence and impartiality that individuals are entitled to expect whenever a decision affecting their rights to privacy and/or freedom of expression is made. Furthermore, as a practical matter, intermediaries have a well-documented tendency
    to remove or otherwise de-link even lawful content for fear of being held liable.[52]
    This ultimately has a chilling effect on free expression.

- **There is a lack of due process safeguards and clarity regarding the "right to be forgotten" which may lead to abuse**, in particular:
  - There is a lack of sufficient information about de-listing requests made to search engines which are successful in the first instance;[53]
  - Original publishers of the information are not required to be notified by search engines about the de-listing requests or about the de-listing decision to enable an appeal where an appeal might be possible; and
  - Search results on the basis of a person's name risk being de-indexed from .com domains where that information might be lawful.

Recommendations

1: Existing remedies should be pursued instead of recognising the "right to be forgotten"

At the outset, ARTICLE 19 wishes to make clear that we do not support nor recommend the recognition of a "right to be forgotten", nor the adoption of dedicated legislation in this area. However, we recognise that it is legitimate for individuals to seek the removal of access to information about them which is either of a private nature (e.g. bank details, medical information, and phone numbers), defamatory, or libellous. In our view, individuals should do so by relying on existing remedies:

- **Privacy and defamation law:** Individuals should apply directly to the courts. Courts are best placed to decide whether the information should remain available because it is justified either as in the public interest as fair comment, or on some other ground.[54] Similarly, the courts are best placed to decide whether any injunction issued against a search engine or Internet service provider is proportionate and does not unduly impinge on the right to freedom of expression.

- **Remedies under the terms and conditions of intermediaries:** Additionally, individuals can use the mechanisms available under the terms and conditions of Internet intermediaries. For example, most social media platforms allow users to flag abusive or harmful content, which then may be removed, following an internal process. This can provide a cheap and effective way to deal with privacy claims without prejudice to ARTICLE 19's recommendation that Internet intermediaries should benefit from immunity from liability.[55]

2: Any "right to be forgotten" should be strictly limited

Where legislation or the courts recognise a legal "right to be forgotten" or it is offered by search engines on a self-regulatory basis,[56] ARTICLE 19 recommends that minimum requirements must be met for such a right to be compatible with the right to freedom of expression, both in terms of substance and procedure. Specifically, the "right to be forgotten" should present the following basic features:

- **Individual right:** The "right" should be limited only to private individuals. The purpose of this right should ultimately be to protect an individual's dignity and privacy, which only individuals are capable of having.

- **A cause of action against search engines:** The "right" should be actionable only against search providers as data controllers rather than against hosting services or content providers. This is because the right has arisen out of a concern that a search for an individual's name generates a public profile of that person. The legality of the underlying publication, therefore, is not at issue, since the publication itself did not create such a profile. Furthermore, the erasure of truthful and otherwise lawful material is problematic for reasons outlined previously.

- **Protecting freedom of expression:** Any protection of the "right to be forgotten" (e.g. in legislation) should make explicit reference to the right to freedom of expression as a fundamental right with which protection must be balanced.

- **The decisions should be issued by courts or independent adjudicatory bodies**: As a matter of principle, the courts or independent adjudicatory bodies (not search providers) should decide whether a "right to be forgotten" request should be granted. At the same time, ARTICLE 19 recognises that search engines are more likely to be the first port of call for such requests. Therefore, it is vital that both parties have the right of appeal to an independent and impartial court or adjudicatory body in disputed cases.

In circumstances where the information subject to a complaint **should never have entered the public domain** in the first place because it was of a private nature and its publication was not otherwise justified, the "right to be forgotten" is not particularly controversial and may offer an alternative to other types of remedies.[57] De-indexing from searches also presents certain advantages over content removal: first, from a pragmatic perspective, it is likely to be more effective than content removal in cases involving hosts based in the United States, who benefit from almost complete immunity for third party content; second, its impact on freedom of expression is less negative than content removal or "takedown" since the information remains available using different search terms.

However, the more controversial aspects of the "right to be forgotten" concern the circumstances in which the **information in question is part of the public record** - whether because, for instance, the individual concerned committed a crime or, in the case of a photo, because it was taken in a public space with no reasonable expectation of privacy, or because the individual consented to the publication of the information at the time but no longer wishes for his or her name to be associated with it. Although we believe that, as a matter of principle, information which is part of the public record should remain in the public domain and be easily accessible by searching for a person's name, we recognise that there might be exceptional circumstances where the public interest in that information may yield to other important interests, such as the rehabilitation of juvenile offenders. Criteria for making determinations on these conflicts are provided below.

3: The strict seven-part test for balancing freedom of expression and the "right to be forgotten" should be applied

ARTICLE 19 believes that the courts or other independent adjudicatory bodies tasked with balancing freedom of expression and the "right to be forgotten" should proceed on the basis that the right to freedom of expression and the right to privacy – from which the "right to be forgotten" is derived - are two fundamental, yet qualified, rights. Under international law, both rights may be limited subject to restrictions under the three-part test of legality, necessity and proportionality. Both rights must be balanced in a fair and proportionate manner without giving precedence to one over the other.[58] In practice, in order to determine whether the balance should tip in favour of either, ARTICLE 19 suggests the situation is assessed under the following seven-part test. Individual criteria are not decisive on their own and, in principle, all parts of the test should be given equal weight.

Test 1: Whether the information in question is of a private nature

The court or independent adjudicatory body should first examine whether the information at issue is of a private nature and should therefore benefit from the protection of the right to privacy. Equally, individuals who wish to avail themselves of the "right to be forgotten" should be required to show that they had a reasonable expectation that the information would remain private. This inherently private information may include:

- Details of their intimate or sex life;
- Information about their health;
- Bank or payment accounts details (such as card numbers);
- Private contact or identification information, including PINs or passwords, passport or social security numbers;
- Other sensitive information such as trade-union membership, racial or ethnic origin, political opinions or religious or philosophical beliefs could also be considered private.

In other words, when the information belongs to one of the above (non-exhaustive) categories, strong justification, such as an overriding public interest in the information at issue, will need to be provided as to why it should remain easily accessible on the Internet through a search for a person's name. For instance, this is unlikely to be the case of "revenge porn" videos, except where a public figure is involved and there is some other sufficiently compelling public interest justification that goes beyond satisfying the public's curiosity.[59]

Test 2: Whether the applicant had a reasonable expectation of privacy

The courts or independent bodies should also assess whether the individual had a reasonable expectation of privacy or forfeited it through his/her actions:

- **Prior conduct:** If any of the above information became public because the individual in question acted in such a way as to forfeit their expectation of privacy, for example because he or she committed a crime or published his or her opinions online, then there should be a presumption that the search results should remain available through a search of their name.[60]

- **Prior consent:** If any of the above information became public because the individual in question consented to its publication, there should be a presumption that the search results should remain available through a search of their name. It should be noted, however, that just because an individual previously consented to the publication does not mean that they necessarily forfeited their right to privacy. Conversely, the absence of explicit consent to the publication of information or photographs should not lead to the conclusion that the publication was not justified. The right to privacy does not require consent to be given in every case prior to publication: to hold otherwise would be both impractical and an unacceptable restriction on freedom of expression.[61]

- **Prior existence of the information in the public domain:** Equally, if the information was already well-known, such as someone's ethnic origin or religious beliefs, on account of his or her profession or public self-declaration, there should be a presumption that the information should remain available through of a search for their name. More generally, the right to private life is unlikely to be engaged if either the information in question had already entered the public domain legitimately or where it had been available publicly for some considerable time, even if it had not entered the public domain in a legitimate manner.[62] Indeed, there should be an overarching presumption that information, which is already legitimately in the public domain, should remain in the public domain.

Test 3: Whether the information at issue is in the public interest

In circumstances where the "right to be forgotten" is engaged because of the private nature of the information at issue, the court or independent adjudicatory body dealing with "right to be forgotten" requests should consider whether there is an overriding public interest in that information remaining available through a search for the individual's name.

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.[63] 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;
- art and culture.

Information about these areas of public concern is therefore likely to tip the balance in favour of the right to freedom of expression.

By contrast, information about purely private matters in which the interest of members of the public is merely salacious or sensational (e.g. links to sex tapes) is unlikely to be in the public interest.[64] At the same time, even intimate details of someone's private life may be considered to be in the public interest if it involves a public figure and/or that person is in a position of trust and there is a wider public interest dimension, e.g. a public figure using public money to fund a lavish private lifestyle.

Test 4: Whether the information at issue pertains to a public figure

The court or other adjudicatory body dealing with "right to be forgotten" requests should also consider whether the information at issue concerns a public figure. There must be a strong presumption that "right to be forgotten" requests submitted by public figures or their representatives should not be granted.

Under international human rights law, public figures, especially leaders of states and elected representatives, have a lesser expectation of privacy than ordinary citizens or even lower ranking public officials.[65] 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.[66] Even if the information at issue has nothing to do with the persons' official duties, it may still be protected by the right to freedom of expression due to the greater public interest in its disclosure or dissemination.[67] In particular, certain facts about the private lives of public figures may be of interest to the public, (e.g. if they revealed a hypocritical approach taken by the public figure in public statements or approaches to public policy).[68] Importantly, public figures also have power and resources that may be used to get negative stories taken down and mislead the public about their true nature. As a result, their requests under "right to be forgotten" should be closely scrutinised.

This does not mean that public figures forfeit all privacy rights: they retain these 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.

Test 5: Whether the information is part of the public record

High profile de-listing requests made on the basis of the "right to be forgotten" tend to concern news articles regarding matters of public interest. Therefore, the nature and origin of the linked information should be considered, in particular:

- **Journalistic, artistic, literary or academic material:** There should be a presumption that links to articles published by individuals or entities engaged in journalistic activity, whether news organisations, bloggers, civil society organisations or other groups performing a public watchdog function, should not be de-listed. The same is true of links to books or academic articles.

- **Government information:** Equally, in circumstances where a government body has published personal information, (e.g. in criminal records, court judgements or bankruptcy filings), and that information has been in the public domain for some time, it would be improper for such information to be de-listed under the "right to be forgotten." As noted above, unless national legislation provides for such information to be expunged after a certain period of time, (e.g. to enable rehabilitation), there should be a strong presumption that the information should not be de-listed.

Test 6: Whether the applicant has demonstrated substantial harm

The court or adjudicatory body examining "right to be forgotten" requests should also assess whether applicants have demonstrated that they have suffered substantial damage or harm due to the availability of the search results linked to their name.[69] Such harm should be more than mere embarrassment or discomfort. Actual harm should be required.[70]

The "substantial harm" criterion is especially important in circumstances where individuals seek the de-listing of links to information of a public nature, or information to which publication they previously consented, or information they themselves made publicly available (e.g. on social media). We believe that in such cases, applicants should be required to show that their privacy is significantly affected by the information remaining easily searchable (through a search for their name).

Finally, as an exception to the above, the "substantial harm" criteria would not necessarily need to be established in the case of children or young persons. Indeed, special considerations should apply in their case. Children have a stronger interest in the protection of their right to private life because of the vulnerability inherent to their age. For this reason, even in cases where there is a strong public interest (e.g. because the information concerns child abuse) there would be strong countervailing interests in protecting children from unwarranted publicity. At the same time, due weight should be given to the age and maturity of children and the fact that their capacity and ability to exercise their own rights increase as they develop.

Test 7: How recent the information is and whether it retains public interest value

Finally, the court or other relevant body should assess the impact of the passage of time on the public interest value of the information at issue and whether it should remain easily discoverable through a search of someone's name.

Information available on the Internet poses new challenges for the balance between the protection of freedom of expression and the "right to be forgotten." A wealth of information available online may be considered trivial in nature (e.g. a conversation on Twitter on mundane topics). Certain information may be of limited intrinsic value when published but it may acquire more significance over time, either because the individual in question may become a public figure, or simply from the perspective of academic, scientific, or historical research.[71] For this reason, it would be simplistic to conclude that links to such information should be de-listed upon request in all cases.

As a general rule, recent information is more likely to have public interest value, and therefore the balance of rights is less likely to be in favour of de-listing the links. At the other end of the spectrum, it is equally clear that links to certain types of information should always remain accessible by searches of a person's name due to the overriding public interest value in them, such as information about crimes against humanity, genocide etc.[72] Similarly, unless domestic law provides for information to be expunged after a period of time (e.g. to enable the rehabilitation of juvenile offenders), information about criminal proceedings should always remain available.

4: Minimum procedural requirements should be observed

ARTICLE 19 also proposes that any "right to be forgotten" requests should be processed in a way that respects the following procedural requirements.

Requirement 1: The courts or independent adjudicatory bodies should decide whether "right to be forgotten" requests should be granted

If countries consider the recognition of the "right to be forgotten," it is likely that, as a matter of practicality, search engines will be required to decide on requests, in the first instance. However, decisions involving complex factual and legal balancing exercises, involving both the right to freedom of expression and the right to privacy, should only be made by a court or independent adjudicatory, not a private service provider.

The fact that search engines may already remove links under intermediary liability provisions elsewhere is not pertinent and ARTICLE 19 has previously criticised such removals on similar grounds.[73] Not only are private providers not equipped to carry out such determinations, but they also lack the necessary guarantees of independence, impartiality, and transparency 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 apply directly to the courts.

Alternatively, it may be appropriate for an independent adjudicatory body to consider such requests. However, we consider that data protection authorities are generally ill-suited to carry out such an assessment due to their inherent institutional bias towards the protection of personal data at the expense of free expression. This is likely to be exacerbated in circumstances where the data protection authority is not independent and such a system would thus be potentially dangerous for freedom of expression in a number of countries.

Requirement 2: Data publishers should be notified and be able to challenge "right to be forgotten" requests

ARTICLE 19 notes that. in practice, the procedure used to give effect to the "right to be forgotten" is likely to present similarities with notice-and-takedown (NTD) mechanisms, for which legislation currently exists in various countries.[74] These place search engines in a position to decide whether to restrict access to content or links, (in the case of the "right to be forgotten"). NTD procedures lack both clarity and fairness.[75] In particular, publishers whose content is removed are not systematically informed that a request has been made to takedown their content in the first place. Therefore they are unable to challenge the request.

While ARTICLE 19 generally opposes NTD procedures, we recommend that in order for them to be 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 that request. If their content is de-listed, they should be given a right of appeal. A process compatible with these principles would therefore be as follows:

- Once a request for de-listing of search results has been submitted by a data-subject, the data controller should make a preliminary assessment as to whether the request meets the formal requirements - that is, whether the claim has prima facie validity;

- If these criteria are met, the publisher of the data at issue should be given notice of the request and the opportunity to submit a counterclaim;

- 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;

- If the data is de-listed, the data publisher should be able to appeal against the decision to an independent public body that would be responsible for dealing with these types of claims, such as a national data protection authority, an information commissioner, or, preferably, the courts.

The above notification requirement, as well as the possibility of appeal, is consistent with a range of international standards, including the Ruggie Principles on Business and Human Rights,[76] and the requirement on states under international human rights law to take positive measures to protect fundamental rights, including between private parties. This principle, which should underpin data protection law, 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.

Requirement 3: De-listings should be limited in scope

In ARTICLE 19's view, if "right to be forgotten" requests are granted, they should be strictly limited to:

- **Search results generated by a search for a person's name:** This is almost always likely to be a more proportionate restriction on freedom of expression than the complete removal of links from search engine databases since the information will at least remain available by way of different search terms.

- **The domain name corresponding to the country where the right is recognised and where the individual has established substantial damage:** It would be improper and in breach of state sovereignty for the de-listing of information to be extended to domain names and/ or countries where that information is lawful. To hold otherwise would have, in our view, a profound chilling effect on access to information worldwide. There is also a significant danger that some governments might use such extra-territorial powers to restrict access to embarrassing information about them.[77]

Requirement 4: Relevant providers, public authorities and the courts should publish transparency reports on "right to be forgotten"

ARTICLE 19 believes that it is vital that relevant providers, public authorities and courts publish transparency reports, including information about the nature, volume and outcome of de-listing requests. This is particularly important with respect to private companies since the law might provide for hefty fines for failure to de-list links in compliance with its provisions. They are therefore much more likely to de-list links, when requested to do so, in order to pre-empt accusations of mishandling personal data.

About ARTICLE 19

ARTICLE 19 is an international human rights organisation, founded in 1987, which defends and promotes freedom of expression and right to information worldwide.

It takes its mandate from the Universal Declaration of Human Rights, which guarantees the right to freedom of expression and information. An increasingly important means of expression and to seek, receive, and impart information is through information and communication technologies such as the Internet. ARTICLE 19 has been promoting the Internet freedoms for over 10 years and is active in developments of policy and practice concerning freedom of expression and the Internet through our network of partners, associates and expert contacts.

ARTICLE 19 encourages organisations and individuals to give us feedback about how this policy brief is being used. Please send your feedback to legal@article19.org.

References

1. Alan Westin, Privacy and Freedom, 1967.
2. Ibid.
3. See, e.g. ARTICLE 19, **Russia: Right to be Forgotten Law**, August 2015.
4. For example, by March 2016, South Korea (see Human Rights Korea, **the Right to be Forgotten in Korea**, August 2014), Brazil (Hunton & Williams, **Brazilian Congressman Introduces Right to be Forgotten Bill**, 23 October 2014; or Lexology, Brazil: Superior Court rejects right to be forgotten and releases search engines from removing search results, 1 December 2014), or Mexico (CNN, **El proceso del IFAI ante Google, un precedente para el derecho al olvido?**, 28 January 2015).
5. See, e.g. European Court of Human Rights (European Court), Handyside v the UK, Appl. no. 5493/72, para 49, 7 December 1976.
6. Article 19 of the UDHR.
7. Article 19 of the ICCPR.
8. Article 9 of the African Charter.
9. Article 4 of the American Declaration.
10. Article 13 of the American Convention.
11. Article 10 of the European Convention.
12. HR Committee, General Comment No.34, CCPR/C/GC/34, adopted on 12 September 2011, para 12.
13. The European Court noted that it "does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life;" see Niemietz v. Germany, 16 December 1992, 16 EHRR 97; see also EPIC and Privacy International, **Privacy and Human Rights**, 2006.
14. See e.g. HR Committee, CCPR General Comment No. 16 on Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988; UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (SR on HR and countering terrorism), A/HRC/13/37, 28 December 2009; see also European Court, Bensaid v UK, App. No. 44599/98 [2001] ECHR 82.
15. Article 12 of the UDHR; Article 17 of the ICCPR, Article 8 of the European Convention, Article 5,9 and 10 of the American Declaration on Human Rights, and Article 11 of the African Charter.
16. See e.g. US Department of State, 2010 Country Reports on Human Rights Practices, April 2011.
17. See e.g. HR Committee, Concluding Observations on Netherlands, CCPR/C/82/D/903/1999 [2004] UNHRC 60 (15 November 2004); Inter-American Court on Human Rights (Inter-American Court), **Escher et al. v. Brazil**, 9 July 2009; or the ECtHR's **summary of European Court case-law on data protection**.
18. US Department of State, 2010 Human Rights Report, op.cit.; Privacy and Human Rights, op.cit; Glasser (ed.), International Libel and Privacy Handbook, 2006.
19. Report of SR on HR and countering terrorism, op.cit.

20. See UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur on FOE), A/HRC/23/40, at paras 24-27.
21. For example, a requirement for newspapers to notify the subjects of a news article before its publication; see European Court, Mosley v the UK, Appl. no. 48009/08, 10 May 2011.
22. See e.g. European Court, **Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland**, Appl. no. 931/13, 21 July 2015
23. Governments and public authorities collect information related to public services and obligations including tax, medical, employment, citizenship and criminal records, whilst technologies for identification including identity card systems, fingerprints, and DNA have quickly evolved and expanded. Private organisations also collect information relating to the use of their commercial or other services and in connection with their marketing and sales activities.
24. See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). Also see US Department of Health, Education and Welfare, Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems July, 1973; Canadian Standards Association (CSA) International, Model Code for the Protection of Personal Information, 1996.
25. **Guidelines for the Regulation of Computerized Personal Data Files**, G.A. Res. 45/95, 14 December 1990.
26. **Commonwealth Secretariat, Model Data Protection Act**. 2002.
27. ECOWAS, ECOWAS Telecommunications Ministers Adopt Texts on Cyber Crime, Personal Data Protection, Press Release No 100/2008, 16 October 2008; or Organisation of Eastern Caribbean States **Privacy Bill (Proposed draft)**, April 2004.
28. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, Strasbourg, ETS 108, 1981.
29. **Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data** (EU Data Protection Directive), Official Journal L 281, 23/11/1995 P. 0031 – 0050, 24 October 1995.
30. The Directive has been adopted by the 28 EU member states, and has been used as a model for the data protection framework of numerous other countries in Europe, Africa, and Latin America that trade with the EU. With the new General Data Protection Regulation (GDPR), the EU is set to establish another blueprint for the protection of personal data around the world.
31. **APEC Privacy Framework**, 2005.
32. See **Case C-131/12, Google Spain v. AEPD and Mario Costeja Gonzalez**, 13 May 2014.

33. See e.g., the **UK Rehabilitation of Offenders Act 1974** or **Article 133-12 ets Penal Code of France**.
34. See e.g., Germany, The Register, **Wikipedia sued for publishing convicted murderer's name**, 12 November 2009. By contrast, in the US, the Court of Appeals for the Second Circuit recently reiterated in a recent Connecticut case that the Erasure Statute did not render tortious historically accurate news accounts of an arrest, see **Martin v Hearst Corporation, 2nd Circuit Court of Appeals, Docket no. 13-3315, 28** January 2015.
35. See e.g. the **Scottish Data Protection Code of Practice on Archival Information**; the **Mexican Federal Law of 23 January 2012 on Archives**, Article 27; **French Code du patrimoine, Livre II Archives**, in particular Chapter 3 on the rules of communication of archival information.
36. The right to truth is particularly developed in the Americas: see Inter-American Commission on Human Rights, **The Right to Truth in the Americas**, 13 August 2014.
37. For example, Argentina, Chile, Peru, El Salvador, Uruguay, Brazil and Guatemala have established Truth Commissions with a view to uncover past human rights abuses; see e.g. Glafira A. Marcon, **Does Brazil have the right to truth?**, The Macalaster Review, Issue 2, Volume 3, 6 February 2013
38. See Inter-American Commission on Human Rights, op. cit., page 18.
39. E.g. Poland, the Czech Republic, Slovakia or Latvia.
40. See Washington Post, **What is lustration and is it a good idea for Ukraine to adopt it?**, 9 April 2014
41. See e.g. Humanity in Action, **Justice or Revenge? The Human Rights Implications of Lustration Policies in Poland**, 2007.
42. See ARTICLE 19, **The Public's Right to Know: Principles on Freedom of Information Legislation**, June 1999.
43. For example, in the EU, the CJEU has recognised the right of individuals to request the de-listing of search results generated by a search of their name, see CJEU, Costeja case, op.cit.
44. For further guidance on the application of the Costeja judgment, see the **Article 29 Working Party Guidelines**, or the **report of Google's Advisory Council**.

45. See the Costeja judgment, op.cit., para 81; ARTICLE 19, **A right to be forgotten? EU Court sets worrying precedent for free speech**, 14 May 2014; or judgments of EU domestic courts highlighting the importance of protecting freedom of expression: Court of Amsterdam decision, C/13/569654, 18 September 2014; Rechtbank Amsterdam, 13 februari 2015, [eiser] tegen Google Inc., ECLI:NL:RBAMS:2015:716 (Amsterdam Court, 13 February 2015, [plaintiff] v. Google Inc., ECLI:NL:RBAMS:2015:716); TGI de Toulouse (ord. réf.), 21 janvier 2015 - Franck J. c/ Google France et Google Inc. (Regional court of Toulouse (under the urgent procedure), 21 January 2015 - Franck J. v. Google France and Google Inc.)

46. For example, in Argentina, celebrities regularly bring actions against search engines for defamation or use of their image without permission in relation to search results appearing on entry of their name; see, e.g. Global Voices Online, **Right to be forgotten: a Win for Argentina's Lawsuit Happy Celebrities?** 18 September 2014). In the Virginia Da Cunha case, a court ordered both Yahoo and Google to pay for moral damage and to remove Da Cunha's photographs from search results related to sex, eroticism and pornography, see Edward L. Carter, Argentina's Right to be forgotten, Emory International Law Review, Vol 27 (1), p.28). The decision was later overturned on appeal, on the ground that intermediaries could not be held responsible for third party content. In Japan, by contrast, injunctions against search engines have been upheld on the basis of personality rights; see, e.g. Matthew Dougherty, **Japan: Google Privacy Case**, DLA Piper blog, 17 October 2014). Failure to comply with such court injunctions is generally subject to civil or criminal sanctions, including severe financial penalties.

47. See High Court, **Contostavlos v Mendahun** [2012] EWHC 850 (QB).

48. See IusComparatum, **Colombia: Constitutional Court rules on the right to be forgotten**, 14 July 2015.

49. This was the case, for instance in the State of California; see e.g. **US: Anti-Revenge Porn Bill and Right to be Forgotten Introduced in California**, IRIS 2013-10: 1/37.

50. See, e.g. Five Rights, available at **http://irights.uk/the-right-to-remove/**

51. **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.

52. See e.g. **https://chillingeffects.org/**

53. While Google provides some information about these requests in its **Transparency Report**, academics have called on Google to do more; e.g. **Dear Google: open letter from 80 academics on 'right to be forgotten'**, 14 May 2015.

54. For instance, where "right to be forgotten"' applications were refused by the courts on the ground that more suitable alternatives existed, see [**http://www.panopticonblog.com/2015/09/18/right-to-be-forgotten-khashaba-revisited/**] and [**http://cyberlaw.stanford.edu/blog/2015/10/no-more-right-be-forgotten-mr-costeja-says-spanish-data-protection-authority**].

55. ARTICLE 19, **Intermediaries: Dilemma of Liability**, 2013.

56. Google has started offering a "right to be forgotten" to victims of revenge porn worldwide, see **Google, Revenge Porn and Search**, 19 June 2015

57. For instance, revenge porn cases are generally better dealt with by way of de-indexing from search or content removal rather than criminal prosecutions, see Lilian Edwards, **Revenge porn: why the right to be forgotten is the right remedy**, Guardian, 29 July 2014.

58. See, the European Court, MGN v. the UK, App. No.39401/04, 18 January 2011, para 142.

59. European Court, **Von Hannover no. 2 v Germany**, App. Nos. 40660/08 and 60641/08 [GC], 7 February 2012, para 110.

60. Mutatis mutandis, European Court, Axel Springer v Germany, App. No. 39954/08 [GC], 7 February 2012, para 83.

61. Mutatis mutandis, European Court, **Mosley v the UK**, App. no. 48009/08, 10 May 2011 in which the European Court held that a requirement to notify the subject of a news article prior to publication would have a chilling effect on freedom of expression and was therefore not required by Article 8 ECHR (right to privacy).

62. Inter-American Court, **Fontevecchia and D'Amico v Argentina**, 29 November 2011, para 17.

63. High Court of South Africa, **Tshabalala-Msimang & Another v Makhanya and Others** (18656/07) [2007] ZAGPHC 161 (30 August 2007)

64. ARTICLE 19, **Defining Defamation: Principles on Freedom of Expression & Protection of Reputation**, July 2000.

65. Inter-American Court, Fontevecchia and D'Amico v Argentina, op.cit.

66. European Court, **Lingens v. Austria, App. No. 9815/82, 8 July 1986**

67. European Court, **Karhuvaara and Iltalehti v Finland**, App. No. 53678/00, 16 November 2004

68. Resolution No 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy: Certain 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.

69. This is also consistent with the jurisprudence of international courts on the relationship between the right to privacy and the 'right to reputation.' In particular, it has been noted that in order to activate the right to privacy, attacks on reputation must attain a "certain level of seriousness" and work "in a manner causing prejudice to personal enjoyment of ... rights;" see European Court, Axel Springer v Germany, op cit. or Court of Amsterdam, C/13/569654, 18 September 2014.

70. 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.

71. **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.

72. Google Report on the Right to be Forgotten, op.cit., page 14; or Inter-American Commission on Human Rights, Cases 11.505, 11.532, 11.541, 11.546, 11.549, 11.569, 11.572, 11.573, 11.583, 11.595, 11.657, 11.705, Report N° 25/98, **Chile, Alfonso René Chanfeau Orayce**, April 7, 1998.

73. ARTICLE 19, Dilemma of liability, op.cit.

74. For example, the E-Commerce Directive in the EU.

75. **Report of the UN Special Rapporteur on freedom of expression**, HRC/17/27, 16 May 2011.

76. **UN Guiding Principles on Business and Human Rights** (also Ruggie Principles), A/HRC/8/5, para 92.

77. ARTICLE 19, **The Right to Forget: EU Privacy Watchdogs Must Protect Freedom of Expression**, 24 July 2014.

DEFENDING FREEDOM
OF EXPRESSION AND INFORMATION

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
T +44 20 7324 2500 F +44 20 7490 0566
E info@article19.org W www.article19.org Tw @article19org facebook.com/article19org