Towards an Internet Free of Censorship II

Perspectives in Latin America

Agustina Del Campo
Compiler

Facultad de Derecho
Centro de Estudios en Libertad de Expresión y Acceso a la Información

CELE

UP
Universidad de Palermo

Towards an Internet Free of Censorship II

Perspectives in Latin America

Agustina Del Campo
COMPILER

Facultad de Derecho
Centro de Estudios en Libertad de
Expresión y Acceso a la Información

CELE

UP
Universidad
de Palermo

Chapter Five

Europe's "Right to Be Forgotten" in Latin America

Daphne Keller[1]

Executive Summary

This article addresses tensions between the so-called "Right to Be Forgotten" (RTBF) and Internet users' free expression and information rights, particularly as those rights are recognized in Latin America. It reviews troubling developments based on two European legal sources: the Court of Justice of the European Union's (CJEU) 2014 *Google Spain*[2] case, which required the search engine to delist certain search results, and the EU's pending General Data Protection Regulation (GDPR).

The GDPR is a once-in-a-generation overhaul of EU Data Protection law. It will come into effect and displace previous Data Protection Law in 2018. Its new RTBF provisions tilt the playing field strongly in favor of erasing online speech, creating a serious imbalance between expression and privacy rights.

---

[1] Daphne Keller is the Director of Intermediary Liability at the Stanford Center for Internet and Society. She was previously Associate General Counsel for Intermediary Liability and Free Speech issues at Google. In that role she focused primarily on legal and policy issues outside the U.S., including the E.U.'s evolving "Right to Be Forgotten." Her earlier roles at Google included leading the core legal teams for Web Search, Copyright, and Open Source Software. Daphne has taught Internet law as a Lecturer at U.C. Berkeley's School of Law, and has also taught courses at Berkeley's School of Information and at Duke Law School. Her extensive public speaking in her field includes testifying before the UK's Leveson Inquiry and Parliamentary Committee on Privacy and Injunctions. Daphne practiced in the Litigation group at Munger, Tolles & Olson and is a graduate of Yale Law School and Brown University.

[2] European Court of Justice, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD),* Case C-131/12, May 13, 2014, at para. 94, available at http://bit.ly/2fbElQH.

Latin American lawmakers and advocates have an opportunity to avoid this imbalance in their own laws. Indeed, there are strong arguments that the GDPR provisions could not pass legal and constitutional muster or comply with human rights commitments in the region. Lawmakers can robustly protect privacy and data protection rights without accepting the harm to speech from poorly designed RTBF laws.

The Article will (1) review the legal background of the RTBF in Europe, and its relationship to other notice and takedown regimes for online speech, (2) discuss the substantive and procedural restrictions to free expression under that law, with a focus on new provisions of the GDPR, and finally (3) identify important differences between relevant EU law and that of many Latin American countries.

The divergences between European and Latin American legal frameworks suggest the following possible approaches for policymakers grappling with RTBF proposals in legislation, litigation, or administrative enforcement:

- Not treating intermediaries as data controllers of speech posted by their users, or spelling out narrower controller obligations with respect to speech.
- Not emulating the removal process set forth in the GDPR, but instead drawing on intermediary liability law to identify any obligations and ensure procedural checks against over-removal.
- Vetting any RTBF proposals against Latin America's unique and pro-free-expression human rights framework.
- Vetting any RTBF proposals against existing legal rights grounded in privacy, defamation, or other sources of law, then identifying whether RTBF would support claims not already covered in those laws, whether those new claims are desirable as a policy matter, and what carefully tailored free expression protections should apply to them.

Introduction

Recent European legal developments in the so-called Right to Be Forgotten fit poorly with legal and human rights frameworks in Latin America. These developments may be of particular concern in the many Latin American countries whose laws track the EU's 1995 Data Protection Directive – the law applied in *Google Spain*.[3] While that case applied only to search

[3] In 2012 this list included Argentina, Uruguay, Mexico, Perú, Costa Rica and Colombia. Leiva, Aldo M., "Data Protection Law in Spain and Latin America: Survey of Legal Approaches", *American Bar Association International Law News*, Vol. 41, No. 4, 2012, available at http://bit.ly/XJ9xyA. In 2016, laws in some 14 countries in Latin America

engines, follow-on cases in the EU seek to apply the same requirement to Internet hosts, such as Facebook. Latin American lawmakers will need to decide similar questions under their own laws. The high level questions arising from these developments will be relevant in every country where lawmakers struggle to reconcile rights to privacy and free expression in online communications.

My own understanding of this issue arises both from my current work at Stanford and from my background as an attorney for Google In 2014, I traveled with the Advisory Council to Google on the Right to Be Forgotten, and heard analysis from both the independent experts who made up that Council and the numerous distinguished speakers who testified at its public meetings.[4] I do not pretend to be an expert in Latin American law. But even a beginner's review of case law and human rights instruments there suggests that the RTBF as it has evolved in Europe would be a poor fit. My hope is that this analysis will be helpful to the region's many remarkable advocates for human rights as national debates about RTBF play out.

I. Discussion

I.A. Legal Origins of the "Right to Be Forgotten" Online

The so-called "Right to Be Forgotten" has longstanding antecedents in European law, for example under German laws designed to help rehabilitated criminals. What was new with the *Google Spain* ruling was the firm grounding of such a right in the EU's broad and powerful Data Protection Directive[5]. The right articulated in that case – to compel search engines to delist certain results for certain search queries – is, many argue, itself no more than a "Right to Be Delisted." It does not compel deletion of web pages or archival materials, and it certainly cannot control human memory. By this reasoning, the RTBF moniker is a misnomer. Nonetheless, the RTBF

and the Caribbean offered some form of Data Protection. Rich, Cynthia, "Data Privacy Laws in the Western Hemisphere (Latin America, Caribbean and Canada)", *Bloomberg BNA - World Data Protection Report*, Vol. 16, No. 6, June 2016, available at http://bit.ly/2fjXULC; there are economic and other reasons to emulate EU law, as the simplest means to be deemed "adequate" for data transfers to national companies doing business in the EU. Cerda Silva, Alberto, "Personal Data Protection and Online Services in Latin America", available at http://bit.ly/2fjY7y9.

[4] Google Advisory Council, *"The Advisory Council to Google on the Right to be Forgotten"*, Final Report, February 2015, available at: http://bit.ly/1r2Vv7e.

[5] Data Protection Directive, available at: http://bit.ly/1f9oJZ7.

terminology has resonated and been repeated around the world, taking on a life of its own beyond the EU legal context.

In Latin America, new cases and legislative proposals advancing RTBF have moved rapidly in the wake of the *Google Spain* case. In some cases, national law already recognizes rights to suppress certain information about one's past, for example in financial or criminal matters.[6] Colombia's Supreme Court in 2015 delivered a nuanced ruling, putting RTBF responsibilities on a web publisher rather than search engines, rooted in part in media law and criminal law.[7] Moreover, many countries' constitutions include *habeas data* provisions, which some argue support rights similar to the EU RTBF.

Questions about the influence of EU law are particularly acute for the many Latin American countries – including Chile, Argentina, Uruguay, Mexico, Costa Rica, Peru, Nicaragua and Colombia - with laws directly modeled on the EU's Data Protection laws, and for countries like Brazil where similar laws have been proposed.[8] Legislatures have significant economic motivation to track EU law, in order to be deemed "adequate" for commercial and other transfer of data from the EU.[9] Latin American Data Protection laws typically include provisions very similar to the ones interpreted in the *Google Spain*, giving data subjects rights to access, rectify, cancel and object to processing of their personal data.[10] Provisions like these were applied by Mexico's Data Protection agency in 2015, in a RTBF order subsequently reversed by a court.[11]

---

[6] Derechos Digitales, "What are the implications of the right to be forgotten in the Americas?", September 2015, available at http://bit.ly/2eL0DNh; See also, Cerda Silva, *supra* note 3 ("For the Supreme Courts of Argentina and Costa Rica, processing personal data on paid debts infringes fundamental rights, whereas for the Supreme Court of El Salvador it does not").

[7] Derechos Digitales, *supra* note 6; *see also* Constitutional Court, "*On behalf of a minor vs. "El nuevo día" newspaper & Instituto Colombiano de Bienestar Familiar"*, Judgment T-453/13, July 15, 2013, available at http://bit.ly/2eAkRJ1 (newspaper, not search engine, liable for disclosing identity of allegedly abused minor); Constitutional Court, *"Martínez vs. Google Colombia & El Tiempo publishing house"*, Judgment T-040/13, January 28, 2013, available at http://bit.ly/1FylMlk (search engine not responsible for accessing, correcting, or deleting search results discussing plaintiff's past criminal process).

[8] Voss, W. Gregory and Castets-Renard, Céline, "Proposal for an International Taxonomy on the various forms of the 'Right to Be Forgotten': a Study on the Convergence of norms", *Colorado Technology Law Journal,* Vol 14, Nº 2, Colorado, University of Colorado Law School, 2016, p. 314.

[9] *See*, Cerda Silva, *supra* note 3. Adequacy determinations made by the European Commission under the 1995 Directive will remain in effect, but could be challenged or revoked in the future under the GDPR. See discussion at http://bit.ly/1FylMlk.

10 Voss and Castets-Renard, *supra* note 8.

[11] *See* http://eleconomista.com.mx/tecnociencia/2016/08/24/anulan-resolucion-inai-sobre-derecho-olvido.

At the same time, some aspects of Latin American law and culture diverge widely from an EU-style RTBF. Eduardo Bertoni, who now heads the Argentine Data Protection agency, called the RTBF moniker "offensive" and wrote that if such a law allowed perpetrators of human rights violations to achieve delisting from Google, it would be "an enormous insult to our history (to put it lightly)."[12] As one Mexican data protection expert put it, "we cannot understand the right to be forgotten as it has been understood by the ECJ because of cultural divides."[13] This divide was already evident in some pre- *Google Spain* case law. For example, in 2013 the Colombian Constitutional Court twice rejected RTBF-like claims against Google.[14]

The region also has powerful case law and legislation protecting the online free expression rights of Internet users, in ways that set it apart from the EU. Implementation of these rights has been inconsistent and in too many cases fallen victim to political corruption, but the intellectual and legal framework remains robust.[15] Brazil's Marco Civil establishes that platforms in most cases need only remove user-generated content if a court has adjudicated it unlawful, and states that this rule is necessary "in order to ensure freedom of expression and to prevent censorship."[16] Chile's Intellectual Property law, too, requires removal only pursuant to court orders.[17] Argentina's Supreme Court arrived at a similar conclusion, reasoning from first principles and constitutional rights. In the landmark *Belen Rodriguez* case, it rejected strict liability, instead predicating intermediary liability on actual knowledge of unlawful content. In dicta, it said that platforms should remove online speech only after adjudication by a competent public authority.[18]

---

[12] Bertoni, Eduardo. "The Right to Be Forgotten: An Insult to Latin American History", *The Huffington Post*, 24th September, 2014, available at http://huff.to/1ucd9pk.

[13] Carson, Angelique. "The Responsibility of Operationalizing the Right To Be Forgotten", The International Association of Privacy Professionals (IAPP), March 12, 2015, available at http://bit.ly/2ek4eRB, quoting Mexican attorney Rosa Maria Franco Velázquez. In striking contrast, the head of Spain's DPA said the RTBF "does not affect the right to know."

[14] Corte Constitucional de Colombia, *supra* note 7.

[15] Some experts have even seen backsliding in recent Inter American Court rulings. *See* http://bit.ly/2hJlGxC.

[16] Federal Law Nº 12.965, April 23, 2014, available in English at http://bit.ly/1gubZiQ.

[17] Law Nº 20.435, May 4, 2010, Art. 85, available at: http://bcn.cl/nol; Chile's Supreme Court also upheld an appellate ruling limiting Internet platforms' obligations to remove allegedly defamatory content, also on grounds of free expression. Supreme Court, "*Suazo vs Reclamos.cl*", 07/06/09. Available at http://bit.ly/2f2LoQT.

18 Corte Suprema de Argentina, "*Rodríguez M. Belen c/Google y Otro s/ daños y perjuicios"*, Judgment R.522.XLIX, 10/28/14. Available at: http://bit.ly/2f2LoQT; India's Supreme Court reached a comparable outcome in "*Shreya Singhal v. Union of India"*, Nº. 167/2012, Criminal Judgment 03/24/15.

This widespread embrace of a court order requirement for Internet content removal stands in contrast to European case law. Most EU countries have consistently accepted notice from interested individuals, without judicial oversight, as an adequate basis for removal of online speech. A partial exception is Spain: Spanish legislation initially required court orders, but the Spanish Supreme Court struck this standard down as inconsistent with the EU-wide eCommerce Directive.[19] A lower court subsequently held that considerations of free expression nonetheless mandated a court order standard, except for legal violations that are "unquestionable, manifest and beyond doubt."[20]

Latin America's special concern for free expression rights is grounded in the region's human rights instruments. Article 13.3 of the American Convention on Human Rights seems to foresee intermediary liability issues of today, saying

The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.[21]

This concern for indirect censorship and private controls is squarely on point for laws that, like *Google Spain*, effectively assign RTBF adjudication to private companies. So, too, are Article 8's guarantee of "competent, independent, and impartial tribunal, previously established by law," and the due process element of the Inter American Court's three-part test for content restrictions.[22]

The Organization of American States' Declaration of Principles on Freedom of Expression is also relevant. It says,

> Privacy laws should not inhibit or restrict investigation and dissemination of information of public interest. The protection of a person's

[19] Tribunal Supremo de Madrid, Sala en lo Civil, "*Asociación de Internautas",* Judgment Nº 773/2009, 11/10/09. Available at http://bit.ly/2f76g8H, discussed at http://bit.ly/2fscOQA.

20 Barcelona appellate court, "*Royo v Google*", Judgment 76/2013, February 13, 2013; a line of UK cases wrangled with the same question, but in many cases addresses it under domestic defamation law rather than eCommerce Intermediary Liability standards. Nonetheless one case, "*Davison v Habeeb",* England and Wales High Court (Queen's Bench Division), November 25, 2011, held that a mere allegation that a user's post was defamatory did not establish knowledge or removal obligation for a blog host.

[21] American Convention on Human Rights, "Pact of San Jose, Costa Rica", available at: http://bit.ly/1Ac82L9.

[22] *See*, Joint Declaration on Freedom of Expression and Responses to Conflict Situations. Available at: http://bit.ly/2gD6F4J

> reputation should only be guaranteed through civil sanctions in those cases in which the person offended is a public official, a public person or a private person who has voluntarily become involved in matters of public interest. In addition, in these cases, it must be proven that in disseminating the news, the social communicator had the specific intent to inflict harm, was fully aware that false news was disseminated, or acted with gross negligence in efforts to determine the truth or falsity of such news.[23]

This framework for privacy-based limitations on speech will be important as signatories of the convention confront RTBF legal proposals.[24]

I.B. Overview of Relevant Data Protection Law

The right established in the EU's 1995 Data Protection Directive, and in many Latin American laws, is distinct from pre-existing privacy rights. It is a broad right to limit processing of all information relating to oneself, not just information that causes harm or invades personal privacy. The EU's Directive sets forth the detailed legal and administrative framework for protecting this right, including specific legal grounds for regulated entities to process personal data about individuals. Where these grounds are not met, processing is unlawful.

Entities that process personal data are generally classified as either controllers or processors. Controllers are, roughly speaking, entities that hold personal data and decide what to do with it. Because they are the decision-makers, they have more obligations under the law – potentially including compliance with erasure or "Right to Be Forgotten" requirements. Processors hold personal data, but follow instructions from a controller about what to do with it. Their legal duties are correspondingly fewer. In a simple example, a firm that holds records about its employees is a controller of their personal information; if it outsources payroll operations under contract with a payroll company, that company is a processor. The CJEU's determination that Google acted as a controller with respect to information indexed in its web search service was a key holding of *Google Spain*.[25]

[23] Principle 10. Available at http://bit.ly/15lje4M

[24] Because privacy rights predate data protection rights in most legal instruments, there are important questions whether older discussions of privacy apply to both. In this case, the answer seems to be yes.

[25] *Id.* at para 82, 85-88.

The CJEU's ruling left open the critical question of the status of other important OSPs, including hosts such as Twitter or YouTube. If those intermediaries, too, are controllers, then the scope of potential Internet speech suppression under the RTBF is significantly broader. There are some strong arguments against this outcome – for example, that hosts cannot be controllers because they only process content at the direction of a user, who is herself the controller. The few cases to date have reached inconsistent results on this question.[26] Free expression-based arguments against RTBF obligations for hosts are also potentially stronger than for search engines, because removing information from a hosting service may eliminate it entirely from the Internet – sometimes leaving even the author with no copy of her work, as occurred with one author's Blogger account in 2016. [27]

I.C. Intermediary Liability Law

The law of intermediary liability limits and defines the legal responsibility of technical intermediaries for content posted online by third parties.[28] Intermediary liability in the EU is governed by Articles 12-15 of the eCommerce Directive,[29] as implemented in the national laws of Member States. Protected intermediaries can range from Internet access providers like Telefonica to social media hosts like Twitter to search indexes like Google, and more.

Under most intermediary liability laws, platforms have no obligations to police user speech, and no liability for unlawful user content they are unaware of. In some legal systems, even knowledge of tortious user expression, including expression adjudicated as unlawful by a court, does not create any legal obligations for the intermediary. The US Communications Decency

[26] Compare "*CG v Facebook Ireland Ltd & Anor*", High Court of Justice in Northern Ireland (Queen's Bench Division), 20 February, 2015, available at http://bit.ly/1f9oJZ7 (Facebook is controller) and Spanish Blogger case, 2015. Available at http://bit.ly/2fezYoK (blog hosting platform is not a controller).

[27] In 2016 an artist reported that Google had deleted 14 years of his work, including his only copies of some, by taking down content he had posted to the company's Blogger service. See "Google's deleted an artist's blog, along with 14 years of his work", *Science alert*, July 18, 2016, available at: http://bit.ly/2aw3Hfw

[28] Latin American laws are discussed above. In the US, key intermediary liability laws are the DMCA 17 USC 512, available at http://bit.ly/24wrfDr and CDA 230 47 USC 230, available at: http://bit.ly/1hlnlbP

[29] European Parliament and of the Council of the EU, Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), June 8, 2000, available at: http://bit.ly/2faazhi

Act Section 230 works this way, and has been credited with facilitating the tremendous economic and technological boom of US tech companies over the past two decades – and with avoiding suppression of lawful speech by cautious or risk-averse intermediaries. In many other countries, removal obligations exist but are limited to protect rights of Internet users.

Many laws, including the EU eCommerce Directive, treat knowledge as a trigger for intermediary action: once the intermediary is aware of unlawful content, it must take it down or face liability itself. Speech platforms typically operate notice and takedown systems to remove user content under these laws. In principle, intermediaries should only remove user content if the legal allegation in the notice is correct and the content actually is illegal. In practice, notice and takedown processes are widely misused to target lawful content, and multiple studies confirm that intermediaries often simply acquiesce to removal requests, including improper ones.[30] Some companies do put real effort and resources into identifying and rejecting unfounded removal requests. I am proud to say that I was part of this effort at Google. But both anecdotal and statistical evidence tell us that such efforts, alone, are often not enough. Information improperly targeted for removal under notice and takedown systems ranges from religious,[31] political,[32] and scientific[33] content to consumer reviews.[34]

The numbers behind this issue are significant. Intermediaries receive a *lot* of bogus removal requests. In the «Right to Be Forgotten» context, Google says that has been asked to delist 1.6 million webpages, and that around 57% of these requests fail to state valid legal claims even under the EU's expansive RTBF law.[35] Microsoft's Bing search engine also reports that over half of the RTBF requests it gets are groundless.[36] Privacy regulators seem to agree: a review of cases brought to national authorities concluded that "in the great majority of cases the refusal by a search engine

[30] *See* list, available at http://stanford.io/2fBMNhk.

[31] Galperin, Eva, "Massive Takedown of Anti-Scientology Videos on YouTube", Electronic Frontier Foundation, September 5, 2008, available at: http://bit.ly/2eRFGzP.

[32] Rodriguez, Salvador, "Russia, Turkey Asked Twitter To Remove Hundreds Of Tweets As Government Censorship Attempts Skyrocket", *International Business Times*, September 2, 2015, available at: http://bit.ly/2fsi7zP

[33] Timmer, John, "Site plagiarizes blog posts, then files DMCA takedown on originals", *Ars Technica*, February 5, 2013, available at: http://bit.ly/2ekn5Ms.

[34] Lee, Timothy B., "Criticism and takedown: how review sites can defend free speech", *Ars Technica*, June 1, 2011, available at: http://bit.ly/2dZl1tg

[35] Google, "European privacy requests for search removals", available at: http://bit.ly/1FdZMGD

[36] Microsoft, "Content Removal Requests Report", available at: http://bit.ly/2faRmwc

to accede to the request is justified."[37]

To counteract the over-removal problem, lawmakers and human rights advocates around the world have developed procedural rules for notice and takedown. Such rules, including penalties for bad-faith notices and opportunities for accused speakers to "counter-notice," are intended to act as a check on over-removal. The Manila Principles, a widely-endorsed "gold standard" for intermediary liability, lists numerous other procedural tools including notice formalities and transparency requirements.[38] This Article will explore the issue of procedural protections for online speech in as they arise in the RTBF context in Section II.B.

I.D. The Collision of Data Protection and Intermediary Liability Issues in the RTBF

Historically, few lawyers have drawn a connection between data protection and the law of intermediary liability. In European practice, the two fields use very different vocabularies, and are for the most part interpreted, enforced and litigated by different practitioners.

The CJEU's 2014 "Right to Be Forgotten" ruling in *Google Spain* changed that.[39] The court determined that Google was a controller of information in search results, with corresponding obligations to curtail processing of that data upon request. The remedy ordered by the court was not complete erasure of the information, either from search results or from Google's underlying indexing infrastructure. Rather, the search engine was required to de-list results only when users searched for the plaintiff's name.[40] The court prescribed what is effectively a notice and takedown system to remove search results, but arrived at this remedy through the language and logic of data protection – with no reference to Europe's intermediary liability rules. *Google Spain* follow-on cases will likely force lower courts to grapple more directly with questions about how the two areas of law fit together.

In 2018, however, the entire framework of Data Protection law underlying *Google Spain* will be replaced by the GDPR. For the first time, the law will mandate specific steps for erasing personal data, including in the RTBF context. It also authorizes extremely high fines - 4% of annual

[37] European Commission Press Release Issued by the Article 29 Data Protection Working Party, Bruselas, June 18, 2015. Available at http://bit.ly/1OoWVnP

[38] Manila Principles, https://www.manilaprinciples.org/

[39] European Court of Justice, *supra* note 2.

[40] European Court of Justice, *supra* note 2, at para. 94.

global turnover or €20 million – against controllers who fail to comply. [41] This financial exposure, combined with legal provisions that are ambiguous at best or highly pro-erasure at worst, makes the GDPR a bigger threat to online speech than the current EU law under *Google Spain*.

The mismatch between Data Protection and notice and takedown systems arises in large part from conflating "back-end," privately stored" user data and publically available speech. Data Protection law was created and evolved largely as a system of rules for back-end data processing – the things your bank, doctor, or health club might do with personal information they hold in their files, for example. For intermediaries, back-end processing includes things like tracking users' online behavior in storage systems such as logs, profiles, or accounts. Data Protection law rightly applies to this kind of data, and provides individuals with access and erasure rights – regardless of whether the company also happens to be an intermediary platform for user generated content. A human-rights-based analysis of erasure requests for back-end data is relatively straightforward. Only two sets of rights are implicated: those of the requesting data subject, and those of the company. Presumably the requester's data protection rights will prevail in most cases. Data protection rules under both the 1995 Directive and the GDPR are broadly reasonable for this two-party situation. Because of the law's historical focus on this scenario, however, the data protection legal framework has few rules and little precedent for addressing public online speech -- the very different data at issue under the RTBF. [42]

Requests for intermediaries to erase *another person's* online expression are very different from a human rights perspective. They affect at least four parties: the requesting data subject; the intermediary; the person who posted the content online; and other Internet users who want to view it. Procedures designed for back-end data deletion and a two-party interaction are not adequate to protect and balance the rights of these four very different parties. When they are applied to online speech, rights to free expression suffer.

II. Free Expression Issues Raised by the RTBF

Human rights lawyers' concerns about RTBF and free expression broadly fall into two categories. The first concerns the substantive right: should

[41] GDPR Art. 83.

[42] One exception is Opinion 1/2008 on Data Protection issues related to search engines - WP 148 (04.04.2008) (distinguishing back-end "user data" from indexed "content data"), p.14. Available at: http://bit.ly/2eo8Ohx

people be able to suppress truthful information about their past, and if so, what limits should be placed on the right? The second is procedural: if a RTBF exists, who should adjudicate its application, and under what rules? In the *Google Spain* ruling and GDPR, EU lawmakers arrived at troubling answers to both of these questions – answers that stand in considerable tension with Latin American legal protections.

II.A. Free Expression and the Substantive Scope of the RTBF

As Eduardo Bertoni has said, the RTBF is a Rorschach test. People project a wide array of meanings onto it. Many of those involve harms already addressed in existing laws governing defamation or other dignitary and reputational harms. Those laws, in Joris van Hoboken's words, "entail intricate doctrines to balance the interests in society in the publicity of and about others and the interests of privacy and dignity of natural persons.[43] For the RTBF, however, those elaborate doctrines, limitations, and defenses do not yet exist. Lawmakers – or Google – are left to reinvent them.

The *Google Spain* court said that Google should remove data that is inaccurate[44] or "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing."[45] This includes truthful information[46] and information that causes no prejudice to the person seeking removal.[47] The Court identified one exception:

> when it appears, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.[48]

The Court did not expand on this public interest balancing test. However, it noted that "as a rule" the public's interest in information does not outweigh

[43] Van Hoboken, Joris, "The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment", Report for the European Commission, Amsterdam, May 2013, at 23. Available at: http://bit.ly/LrCKYE

[44] European Court of Justice, *supra* note 2, para. 92.

[45] *Id.* at para. 94 (paraphrasing Directive Article 6.1(c)).

[46] *Id.* at para. 92.

[47] *Id.* at para. 96.

[48] *Id.* at para. 97.

the data subject's rights to erasure.[49] In an omission that is striking to many human rights advocates, the Court did not identify or discuss the other affected free expression rights: those of the webmaster or publisher.[50] The ruling was widely criticized both for setting a vague standard and for elevating data protection rights above information access rights, rather than weighing them equally. As former UN Special Rapporteur for Freedom of Expression Frank La Rue, a Guatemalan human rights attorney by training, explained:

> The right to privacy and to data protection is a fundamental right intimately linked to the exercise of the right to freedom of expression, and they should be understood as complementary and never in conflict with each other. The right to be forgotten, as such, does not exist… The decision of any authority to delete information or to block search engines can only be based in the fact that the form of obtaining such information or the content of such is malicious, is false, or produces serious harm to an individual.[51]

La Rue's formulation draws on important substantive limits in pre-*Google Spain* law – and in the Inter-American Convention -- protecting speech that is not malicious, false, or harmful. This approach stands in striking contrast to the CJEU's expansive standard, which allows deletion of truthful and non-prejudicial information.

La Rue also linked RTBF law to issues of political violence and human rights abuses.

> In the case of human rights, one of the fundamental principles to eradicate impunity is to establish the truth of human rights violations when they exist, and this is recognized as the right to truth of the victims and their families but also to society as a whole to reconstruct historical memory, to memorialize the victims of the past.

Despite concerns raised by La Rue and others, new RTBF provisions under the GDPR do little to improve on the CJEU's guidance. The law ex-

[49] *Id.*

[50] *See* Peguera, Miquel, "The Shaky Ground of the Right to be Delisted", on: *Vanderbilt Journal of Entertainment & Technology Law*, Vol. 18, Nº 3, 2016, p. 555. Available at: http://bit.ly/2ghbOMB. Because the CJEU does not accept amicus or intervener briefs, and the newspaper that published Mr. Costeja's information could not be a party. No one before the court directly represented those interests.

[51] Google Advisory Council, *supra* note 4.

cuses controllers from erasing information needed "for exercising the right of freedom of expression and information."[52] But it defers to EU Member State law to define what those rights actually are, and how to balance them with data protection rights.[53] EU Member States have already had this obligation for two decades under the 1995 Directive, and many have failed to fulfill it.[54] Some countries have never passed the required legislation at all, others have enacted laws that fall far short of the goal of balancing expression and privacy rights.[55]

In addition, some GDPR protections extend only to journalistic, artistic, academic or literary expression. This formulation is not unique to EU law, but it is a problem for democratic participation in online speech. Most Internet users lack the credentials to qualify for these limited exemptions. Important content left unprotected under this standard could include consumer reviews of dangerous business practices and first person accounts of abuse by family members or people in positions of power.[56]

More problems arise from institutional imbalance in government support for data protection rights and free expression rights under the GDPR. A person asserting data protection rights has an audience and presumptive ally in the DPA, which can provide inexpensive and efficient enforcement for valid claims. By contrast, the legal avenues available to a publisher or online speaker asserting free expression rights against RTBF removals under European law are scant. In most cases, her only recourse is to courts of law, where she can attempt to sue either the intermediary or the data subject who requested removal. Neither claim is likely to succeed – in most cases there is no clear cause of action against an individual whose false accusation led

[52] Art. 17.3. Notably, this provision does not change OSPs' obligations to immediately "restrict" content from public before assessing whether a free expression defense might apply. See Section II.B. below.

[53] Art. 85.

[54] *See* Erdos, David, "Fundamentally Off Balance: European Union Data Protection Law and Media Expression", Research paper Nº 42/2014, University of Cambridge, Faculty of Law, July 25, 2014. Available at: http://bit.ly/2fgRXfc

[55] *Id*, p. 11. "The laws of three countries (Croatia, Czech Republic and Spain) provide no media derogation at all from any part of the data protection scheme".

[56] The GDPR also importantly lacks clarity about *whose* free expression rights matter: the intermediary's or the user's. While most free expression advocates would identify the user as the most important rightsholder, EU caselaw – including the *Google Spain* ruling – has sometimes looked solely to the rights of defendant OSP. *See* Keller, Daphne, "Litigating platform liability in Europe: new Human Rights case law in the Real World", *The Center for Internet and Society Blog*, Stanford Law School, April 13, 2016, available at: http://stanford.io/2fFmxyG

an intermediary to remove content, or against the intermediary for taking that accusation at face value.

The GDPR's cumulative disadvantages to speech rights would be relatively harmless if data protection law still primarily applied to back-end data held and processed internally by companies. Applying the same rules to Internet users' public online expression, however, strips them of robust protection for their online participation and speech. Jurisdictions in Latin America can provide that protection, without compromising data protection or privacy rights under their own national law.

II.B. Procedural Protections For Free Expression and the RTBF

One important critique of the *Google Spain* ruling was that it effectively put decisions balancing European users' speech and privacy rights into the hands of foreign technology companies, instead of national courts. Of course, such decisions are already put in private hands under many existing Intermediary Liability laws. As discussed above, well-crafted notice and takedown laws can temper the risk to online expression by imposing procedural checks on over-removal. For example, Chile's Intellectual Property law establishes procedures to notify the accused infringer when someone asks to remove her content, and allow her to "counter-notify" to defend against the accusation.[57]

The CJEU's *Google Spain* decision did not prescribe any particular process for Google to follow in assessing and acting on RTBF claims. The Court did not reference Intermediary Liability laws under the eCommerce Directive, perhaps because it is widely assumed in the EU that those provisions do not cover data protection.[58] Subsequent opinions by data protection regulators have added modest procedural improvements, but nothing approaching the robust notice and takedown rules endorsed in many countries' Intermediary Liability laws.[59] The GDPR will introduce procedural rules that are considerably worse -- replacing existing uncertainty about notice and takedown processes for RTBF with a novel process that lacks even basic

[57] Law No. 20.435, May 4, 2010, amending Intellectual Property Law, Art. 85U.

[58] This complex point of EU law is discussed in my forthcoming article. Disputes stem in part from eCommerce Directive language stating that it does not apply to questions covered by the Data Protection Directive. Art. 1.5(b). *See* Data Protection Directive *supra* note 5.

[59] Article 29 Data Protection Working Party. "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12". Adopted on November 26, 2014. Available at: http://bit.ly/1rz3sgx.

procedural protections for online speech.

The GDPR, a comprehensive update and reform of the 1995 Data Protection Directive will come into force on May 25, 2018. Because it is a Regulation rather than a Directive, it will not have to be implemented as separate legislation in each member state of the EU. Rather, it will automatically go into effect. The GDPR covers a lot of ground, with provisions addressing everything from data transfer, to company codes of conduct and appointment of data protection officers.

The GDPR is riddled with ambiguities, including in the RTBF provisions. Some perpetuate existing, unresolved questions under the 1995 Directive. Others are new. We are unlikely to see expert consensus anytime soon about everything the GDPR means. On the upside, this creates openings for litigation and policy advocacy regarding the GDPR's impact on Internet intermediaries and user free expression. On the downside, it leaves Intermediaries with unclear instructions, coupled with powerful financial incentives to assume the most conservative interpretation of both substantive and procedural rules about RTBF removals.[60] Since only intermediaries – not the accused speakers – know about the request and can participate in DPA proceedings, this in turn reduces the chances for DPAs or courts to review improprieties and adopt interpretations more favorable to free expression.

The GDPR's notice and takedown rules must be derived from scattered sections throughout the document. Close evaluation shows a removal process like this. Considerably more detail about the GDPR process can be found in my forthcoming article, or in blog posts on the Stanford CIS website.[61]

1. An individual submits a removal request. There are no specific requirements for information the individual must provide to substantiate her request or confirm it does not conflict with the public interest.[62]
2. In most cases, prior to assessing the request's legal validity, the intermediary temporarily "restricts" the content so it is no longer publicly available.[63]

[60] Fines can mount to 4% of annual global turnover or €20 million. Art. 83.

[61] Keller, Daphne, "Series conclusion and summary: intermediaries and free expression under the GDPR, in brief", *The Center for Internet and Society Blog*, Stanford Law School, December 1, 2015, available at: http://stanford.io/2fFtX4U; *See also* the Spanish-language summary of final GDPR RTBF provisions: http://stanford.io/2fFogE7

[62] *See* generally Art. 17.1(c) and Art. 12.3-12.6. By contrast, Chile's Intellectual Property Law specifies formalities and required information for removal requests. *See* Law No. 20.435, *supra* note 57, Art. 85 Q.

[63] Art. 18.

3. The intermediary reviews the requester's legal claim to decide if it is valid. For difficult questions, the intermediary may be allowed to consult with the user who posted the content.[64] The GDPR identifies free expression rights as a factor in this decision, but adds no guidance on balancing these against data protection rights.[65]
4. For valid claims, the intermediary proceeds to "erase" the content.[66] There is no indication that this "erasure" can ever mean less than 100% deletion, although the *Google Spain* precedent would seem to support less drastic action. For invalid claims, the intermediary is supposed to bring the content out of "restriction" and reinstate it to public view. There are no apparent consequences if it doesn't reinstate the content.
5. The intermediary informs the requester of the outcome, and communicates the removal request to other controllers processing the same data.[67]
6. If the intermediary has information about the user who posted the now-removed content, it seemingly must disclose it to the individual who asked for the removal.[68]
7. In most cases, the accused publisher receives no notice that her content has been removed, and no opportunity to object. The GDPR text does not spell out this prohibition, but does nothing to change the legal basis for regulators' conclusions on this point in the *Google Spain* context.[69]

The deviation from standard notice and takedown processes here is significant, and dangerous for Internet users' expression and information-access rights.

One of the biggest issues with the GDPR process is Step 2: the immediate, temporary "restriction" of content from public view. There are arguments an intermediary could invoke to skip this step in special cases, but it is very unclear whether those arguments could prevail – and raising them would be an expensive risk for intermediaries.

The restriction provisions shift an important default: from a presumption that online expression is permitted until proven otherwise, to a presumption that its challenger is right. This conflicts with both standard legal protec-

[64] This authorization is not spelled out in the GDPR, but it re-uses language from the 1995 Data Protection Directive, which regulators have interpreted to establish these rules. *See* Article 29 Data Protection Working Party, *supra* note 59, p. 3, para. 9.

[65] Art. 17.3.

[66] Art. 17.1.

[67] Art. 17.2 and Art. 19.

[68] Art. 14.2(f) and 15.1(g).

[69] Article 29 Data Protection Working Party, *supra* note 59, p.3.

tions for free expression[70] and with our best knowledge about real-world RTBF requests - recall the 57% bogus notice rate reported by Google. An allegation made in secret to a private company should not have such drastic consequences. The GDPR's "restriction" requirement might make sense when applied to back-end data stored and used by companies. But where notice and takedown applies to third parties' online speech, that speech deserves far better protection.

The GDPR also creates considerable procedural unfairness in Step 6, in most cases preventing the user who posted the disputed content from knowing that it has been removed or delisted. Notice to the affected user is important to deter over-removal in the GDPR context, particularly for smaller intermediaries with scant legal resources. One of the main purposes of such notice is to let affected users correct the *intermediary's* errors, as well as the notifier's errors. Routinized notice puts the opportunity for error-correction in the hands of the person best motivated and equipped to use it: the content's publisher. Leaving the determination entirely in the hands of a technology company simply cannot substitute for involving the publisher as a mechanism to reduce improper removals.

From a pure data protection perspective, leaving the accused publisher out of the loop makes a sort of sense: if an individual has the right to make the company stop processing data about her, which should also preclude their talking to the publisher about it. This "when I say stop, I mean stop" reasoning may be sensible for stored, back-end data. But when the free expression rights of another individual are at stake, systematically depriving that individual of any opportunity to defend herself is a serious denial of fairness and due process.

Finally, the GDPR's seeming requirement that intermediaries disclose personal data about accused speakers is remarkable. It, too appears to be an artifact of rules intended for back-end data, listing Controllers' obligations when they receive data about an individual from someone else. Controllers must tell the data subject "from which source the personal data originate"[71] and "any available information as to their source."[72] The GDPR makes no reference to subpoenas or other forms of valid legal process for Controllers

[70] In a notable exception, a pre-Marco Civil Brazilian ruling held that a hosting platform must, within 24 hours of receiving a notice, temporarily remove user content pending legal analysis of the notifier's claim. Superior Court of Justice, Third Panel, Google Brazil, Special Appeal No. 1323754/RJ, August 28, 2012.

[71] 14.2(f).

[72] 15.1(g)

who receive data in the form of users' speech to protect those users' own private data.

Presumably, such an obligation will look as unreasonable to privacy regulators as it does to civil liberties advocates, and they will find some way to avoid it. Notably, Latin American lawmakers would face the same issue, under their existing data protection law, if they followed the *Google Spain* precedent and treated intermediaries as data controllers for users' speech. Laws in Chile, Colombia, and likely other countries requires controllers outside the journalistic context to disclose the source of personal data.[73]

III. Questions about the Google Spain ruling for non-EU countries considering RTBF laws

These developments in EU data protection law have ramifications for countries outside the EU. Questions about following in the footsteps of EU law will be intensified as the GDPR comes into effect.

From a human rights perspective, this is a complex question. On one hand, EU law has been admirably robust and innovative in protecting Internet users' privacy rights. There are good reasons that advocates might want to emulate many of its choices. On the other hand, the way the RTBF has played out in Europe gives far shorter shrift to speech rights than many other legal systems would do. And, simply as a matter of doctrine and blackletter law, EU developments were driven in part by rules unique to Europe, with no corollary in Latin America. Below is a list of considerations relevant to policy development outside the EU.

III.A. Does the *Google Spain* ruling compel identical interpretation of other countries' legislation that resembles the Data Protection Directive?

Of course, national courts will interpret their own national laws, and not assume that the CJEU ruling makes sense for their own countries. However, to the extent that EU precedent is relevant, it is important to recognize that the CJEU's interpretation was by no means a foregone conclusion, even under EU law. The CJEU's own Advocate General for the case, in fact, recommended

[73] *See* DLA Piper, "Data Protection Laws of the World", 2016, available at: http://bit.ly/2fvYkMx. Interestingly, a Chilean appeals court identified data protection law as a reason not to disclose online speakers' information in a case rejecting defamation liability for an Internet host. Supreme Court, *Suazo vs Reclamos.cl*, 6/07/09, *supra* note 17.

the opposite outcome: that Google was not acting as a controller, and that in any case the Data Protection Directive did not support a right to delete public information based on personal preference.[74] Numerous data protection specialists criticized the court's analysis in the aftermath of the case. Criticisms based on Free Expression concerns may be the most important grounds for other countries to choose a different course, from a human rights perspective. However, purely doctrinal critiques are also relevant for countries with EU-like laws. For example, classing an intermediary as a data controller is difficult to reconcile with some key obligations of controllers – obligations that are effectively impossible for intermediaries to meet. For example, controllers must get consent or other special authorization before processing data about someone else's health, ethnicity, sexual orientation or other "sensitive" attributes. For open speech platforms accepting users' statements about other people, this is effectively impossible.[75] Requirements to give data subjects notice prior to "collecting" data about him are also nonsensical when the "collection" consists of letting a user freely post expression online.[76]

These concerns could readily support the legal conclusion that intermediaries are *not* controllers of user-generated content. Alternatively, it could support the conclusion that they become controllers, and take on removal obligations, only after adequate and substantiated notice. The Italian Supreme Court reached exactly this conclusion in a pre-*Google Spain* case.[77] Framing the issue this way would protect important privacy values. It would preserve entirely Internet users' data protection rights regarding back-end tracking or profiling data. Moreover, it would permit lawmakers to apply their existing notice-and-takedown frameworks, including free expression protections, to users' online speech.

III.B. What is the "Right to Be Forgotten"?

As discussed above, the right adopted by the CJEU in Google Spain was a right to be delisted from certain web search results. Whether some version

[74] Opinion of Advocate General Jääskinen, European Court of Justice, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD),* Case C-131/12, May 13, 2014, para. 20, available at http://bit.ly/2fbElQH

[75] *See* discussion in Peguera, *supra* note 50.

[76] Several Latin American Data Protection laws, including Mexico, Colombia, and Argentina, have versions of this requirement. *See* DLA Piper, *supra* note 73.

[77] Italian Supreme Court of Cassation, "*Milan Public Prosecutor's Office v. Drummond*", Judgment Nº 5107/14, December 17, 2013, available at: http://bit.ly/2efrUYY, at para.7.4 (informal translation).

of this right applies to other sources of information, including the websites themselves, is very much an open question. Extending the right beyond search results would have serious consequences. As advocates consider RTBF proposals in other countries, clarity about the scope of online or offline speech affected by any such right will be critical.

III.C. Should intermediary liability law shape RTBF outcomes outside the EU?

The connection between conventional Intermediary Liability law and RTBF Notice and Takedown practice is conceptually simple. The free expression considerations are the same, from the affected online speaker's perspective, regardless of the legal framework that suppresses her speech. In Europe, however, a major legal barrier complicates this question. The eCommerce Directive, which governs all other aspects of EU Intermediary Liability, says "[t]his Directive shall not apply to (…) questions relating to information society services covered by" data protection law.[78] This leads many – though by no means all - EU lawyers to conclude that RTBF falls outside of ordinary notice and takedown rules. That carve-out, if it exists, is uniquely European. It should not preclude countries outside the EU from drawing on their own Intermediary Liability laws.

A more complex issue is whether controllers' duty to erase personal data is truly a form of "liability" for third party content, or instead their own independent obligation. However, this question, too, is subject to different laws and considerations in different countries. For jurisprudence that frames Intermediary Liability rules as a form of speech protection there is little reason to vary that protection depending on legal conceptions of "liability."

III.D. Is the CJEU's analysis of fundamental rights consistent with human rights obligations and constitutional law in my country?

The CJEU suggested that privacy or data protection rights should, "as a rule," trump the public's rights of access to information. This conclusion was widely criticized by EU lawyers, but stands as law for RTBF removals under *Google Spain*. This prioritization of privacy rights over speech rights is clearly incorrect in some other systems, including the

[78] eCommerce Directive, Article 5.1(b), *see* also Recital 14.

Inter-American system of human rights. That difference is relevant for both of the RTBF's free speech issues: the scope of the substantive right, and the procedural rules for Internet companies as adjudicators of online speech. Differences could also arise from the way national constitutions define and delineate rights. Data protection, as a right distinct from privacy, is a fundamental right under the EU Charter. Latin American practitioners in countries with constitutional *habeas data* rights,[79] and in countries that constitutionally protect only traditional privacy rights, will face important questions about balancing these rights under their own constitutional systems.

III.E. Does existing national law already protect privacy and dignity rights online?

Where existing law already gives people instruments to protect their privacy, reputation, dignity, or honor, or to prevent discrimination based on personal information, it is important to question what would be added by adopting a RTBF.[80] Adding a new, ill-defined RTBF, untethered from the nuanced claims and defenses in existing laws, may only muddy the waters and increase frivolous claims and over-removal of online content.

If lawmakers do see shortcomings in existing law, it can be remedied with more tailored laws incorporating protections for free expression – without invoking the blunt instrument of EU-style RTBF laws.

III.F. Does the EU already apply its Data Protection law to online expression in my country anyway?

In the *Google Spain* case, one of the key rulings was jurisdictional – that EU law applied to data processing carried out outside of Europe by the American Google parent company, because of connections between web search and advertising sales carried out by the local subsidiary. Many experts believe the 1995 Directive also applies to foreign companies on other grounds.

[79] These include, with some variation, Argentina, Brazil, Colombia, Mexico, Peru, and Venezuela. Cerda Silva, *supra* note 3.

[80] Notably, in the wake of the *Google Spain* ruling, many existing claims to intermediaries and courts making claims under defamation of or other sources of law were refiled as data protection claims. Hurst, Ashley. "Data Privacy and Intermediary Liability: Striking a balance between privacy, reputation, innovation and freedom of expression", part 1. Available at: http://bit.ly/2fxRXXu. (Noting that using data protection claims in lieu of privacy or defamation avoids "lengthy debate about such terms as "reasonable expectation of privacy" and gives plaintiffs "a potential short cut")

Whatever the answer is under that law, the GDPR clearly expands extra-territorial application to Internet companies around the world – including both processors and controllers- as long as they "monitor" EU users.[81] "Monitoring" seems to encompass online accounts and standard web and app customization features, so the law reaches many online companies outside of the EU. In addition, regulators have asserted that these companies must delete content globally – including in countries where that content is protected by free expression laws. This assertion of jurisdiction puts both foreign companies and foreign lawmakers in an awkward position, as they wrangle with compliance choices and EU diplomatic and commercial relations.[82]

In practice, EU regulators presumably will not prioritize or dedicate limited resources to policing small and distant companies. However, the GDPR will be an issue for companies with growing EU user bases and presence in Europe.[83] They will need to think hard about their obligations under the Regulation overall – not just its RTBF requirements. (There is an interesting question about authority running the other way: should non-EU data processing laws, including potentially more liberal rules balancing free expression, govern European processing?)

III.G. Can administrative agencies adjudicate free expression rights under my country's legal framework?

By extending data protection law to cover public online expression, the Google Spain ruling moved considerable new authority into the hands of data protection regulators. These administrative agencies can decide whether certain information will be possible to find using search engines. If RTBF is extended to hosting platforms, the same regulators will determine whether expression appears online at all. Resting such power in the hands of administrative agencies, rather than courts, may be permissible under the EU's law and human rights framework. Policymakers in other countries, however, may reach other conclusions.

[81] Art. 3.2(b).

[82] Keller, Daphne y Brown, Bruce D., "Europe's Web Privacy Rules: Bad for Google, Bad for Everyone", *The New York Times*, April 25, 2016, available at: http://nyti.ms/2fpm3f2.

[83] Another new jurisdictional hook covers foreign entities "offering goods or services" in the EU. In a recital, however, this ground is cabined based on factors such as the national currency used for prices. R. 23. Recitals in the GDPR also evince a real frustration with claims that EU law does not reach the foreign corporate parents of subsidiaries established in the EU, saying "legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor" for determining "establishment" jurisdiction under Article 3.1.

Conclusions and recommendations

Grounding a RTBF in EU-style data protection law leads to imbalanced rules that under-protect Internet users' free expression rights. One remedy for this, in the EU and elsewhere, would be to incorporate significant new substantive and procedural protections for speech within data protection law. A simpler approach, however, is to recognize that obligations for intermediaries to erase online speech are very different from obligations for them to erase back-end user data. The issues raised by speech deletion, and the need for procedural rules that protect against over-removal, are already addressed in intermediary liability laws and in free expression jurisprudence.. Those rules can be brought to bear in protecting both speech rights and privacy and data protection rights.

Lawmakers concerned with protecting the full spectrum of rights have many doctrinal options under their own national laws. While these will vary by country, the considerations identified in this article can help lawmakers and human rights advocates in arriving at robust legal frameworks to protect the rights of Internet users.