The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation

Daphne Keller
Stanford Law School Center for Internet and Society
February 8, 2017

TABLE OF CONTENTS

I. Introduction

A. Issue Overview

Two strikingly different areas of law are currently reshaping Internet users' rights to seek and impart information on the Internet. The first, Intermediary Liability, focuses on the legal responsibility of Online Service Providers (OSPs) for their users' speech, and is a key source of protection for individual expression and information rights on the Internet. The second, Data Protection, focuses on information about individual people. It gives them legal rights to limit the ever-proliferating uses of their personal data, both online and off. Both sets of laws protect fundamental rights and preserve Internet services as, in the words of the European Court of Human Rights (ECHR), "essential tools for participation" in contemporary society and public life.[1] But they do so through profoundly different legal frameworks.

The two fields of law came together with a bang in 2014, when the Court of Justice of the European Union (CJEU) endorsed a so-called "Right to Be Forgotten" (RTBF) under EU Data Protection law. In the *Google Spain* case, it ruled that Google must honor claimants' requests to exclude certain search results when users searched for the claimant's name.[2] The right the Court established, which might more accurately be termed a right to "de-list" information from search engines, was not absolute. The claimant's rights had to be balanced against those of other people, including other Internet users looking for information online. Rather than have European courts strike this balance on a case-by-case basis, the CJEU placed de facto adjudication power in the hands of Google, requiring the company to assess each de-listing request and decide whose rights should prevail.

---

[1] Ahmet Yildirim v. Turkey, App. No. 3111/10, E.Ct.H.R. (Dec. 18, 2012) para 54,

[2] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos 2014 O.J. C 212/4 at Rul. Par. 3 http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN, [hereinafter *Google Spain*].

The legal obligations created by *Google Spain* have been well examined in the academic, popular, and professional literature.[3] But these obligations are about to change. In 2018, the EU's new General Data Protection Regulation (GDPR) will bring an enhanced RTBF to Europe – and, through expansive jurisdiction provisions, to the rest of the world.[4]

As this article will discuss, the GDPR locks in language and processes rooted in Data Protection that fit poorly with OSPs' function as platforms for communication. It couples unclear content erasure obligations for OSPs with unusually powerful compliance incentives – including potential fines as high as 4% of annual global turnover or €20 million.[5] Unless lawmakers establish rules or guidelines limiting the law's impact, OSPs will have good reason to honor not only legitimate RTBF requests, but also abusive or mistaken ones, removing information the public has every right to see. Over-reaching RTBF requests that Google has reported receiving already include claims from public officials trying to suppress old criminal records, priests wanting to disguise a history of sexual abuse in their parishes, and financial professionals attempting to hide convictions

---

[3] *See, e.g.*, Jef Ausloos and Aleksandra Kuczerawy *From Notice-and-Takedown to Notice-and-De-list: Implementing the Google Spain Ruling*, 14 COLO. TECH. L.J. (Forthcoming Spring 2016) at 14 (hereinafter *Ausloos and Kuczerawy*); Stefan Kulk and Frederik Zulderveen Borgesius, *Google Spain v. González: Did the Court Forget about Freedom of Expression?*, 5 EUR. J. RISK REG. 389 (2014); Miquel Peguera, *The Shaky Ground of the Right to be De-listed*, 18 VAND. J. OF ENT. & TECH. L. 507, 539 (forthcoming 2016); Joris van Hoboken, *Case Note, CJEU 13 May 2014, C-131/12 (Google Spain)* (2014), https://ssrn.com/abstract=2495580; Christopher Kuner, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges*, in Burkhard Hess and Cristina M. Mariottini (eds.), Protecting Privacy in Private International and Procedural Law and by Data Protection, 19-55 LSE Legal Studies Working Paper No. 3/2015; Farhad Manjoo, *'Right to Be Forgotten' Online Could Spread*, NY TIMES (Aug. 5 2015), https://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html.

[4] Commission Regulation 2016/679, 2016 O.J. (L119) 1(EU) (hereinafter *GDPR*); European Commission, *Reform of European Data Protection rules*, http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

[5] GDPR Art. 83.5(b). As discussed in *infra* Section III.A, more sophisticated OSPs will likely be advised to expect far lower fines, but most OSPs will not have access to such expert advice.

for defrauding clients.[6] Both Google and Bing report that over half of the de-listing requests they receive state claims that, like these, are not valid under European laws.[7]

This pattern of over-reaching requests should come as no surprise. Abusive removal demands are a problem in every notice-and-takedown system – and studies suggest that OSPs comply with them all too often.[8] No matter what one thinks about the proper scope of legitimate de-listing or removal requests, the abusive ones are a problem. Relying on a US technology company to resolve delicate questions of national law affecting Internet users' fundamental rights is also a problem. But they are not new problems, or intractable ones. They arise over and over in the context of Intermediary Liability – the law that shapes OSPs' obligations for other claims, like copyright infringement or defamation. Europe's own existing Intermediary Liability laws, along with guidance from human rights bodies and civil society, provide tools to solve them.[9] In particular, procedural rules for OSPs' notice-and-takedown operations can, like procedural rules in litigation, make the process fairer for all sides and increase the likelihood of just outcomes.

This article is about using those tools to help the GDPR achieve its real goals: balancing and protecting *all* rights, including both privacy and information rights. It will closely examine the GDPR's new notice-and-takedown rules and argue that they are, on their face, dangerous to information rights and to the Internet as an open platform for democratic participation. It is possible, however, to interpret the GDPR in light of

---

[6] *See* generally Google Transparency Report, https://www.google.com/transparencyreport/removals/europeprivacy/.

[7] *Id*.; Microsoft Content Removal Requests Report, https://www.microsoft.com/about/csr/transparencyhub/crrr/. DPAs reviewing de-listing claims rejected by the companies concluded that "in the great majority of cases the refusal by a search engine to accede to the request is justified." This suggests that the self-reported 50% rate of improper requests is roughly accurate by regulators' standards. Article 29 Data Protection Working Party, Press Release (June 18, 2015) http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20150618_wp29_press_release_on_delisting.pdf.

[8] *See* Section II.A.

[9] *See Ausloos and Kuczerawy*, *supra* note 3, at 14 (observing this point and suggesting procedural protections) (noting, "[b]eing the subject of discussions for over a decade, the lessons learned in the notice-and-takedown context might prove particularly useful for implementing the right to be de-listed").

fundamental rights considerations and arrive at a more balanced set of rules. The Article presents a proposed analysis for practitioners and lawmakers seeking to do so.

This Article is emphatically not about two other, related issues.

First, it is not about the underlying substantive legal right to "be forgotten" by obscuring or erasing truthful information about oneself. My contention is not that such laws are good or bad. Every legal system has laws that limit expression rights to protect privacy, and vice versa. Advocating for a particular version of this difficult balance is not the Article's point. Instead, it focuses on procedural fairness. Without well-designed notice-and-takedown rules, no matter what expression the law says to delete, we should expect OSPs to delete more.

Second, this Article is not about the data that OSPs collect by tracking their own users' online behavior. OSPs have plenty of this privately held, "back-end" data - logs tracking users' clicks, profiles used to target advertisements, and more. Data Protection laws, including erasure obligations, rightly apply to this back-end data. This Article does not dispute Internet users' rights under the GDPR to make OSPs to erase data of this sort. Accordingly, I will use the term "RTBF" to refer only the right to erase or de-list information put online by another Internet user.

I bring a particular perspective and history to this issue. Until 2015 I was an Associate General Counsel for Google. For much of that time, I was the lead lawyer for the company's web search service and grappled with speech and Intermediary Liability laws around the world. In my final months with the company, I traveled with the independent Advisory Council convened by Google to advise the company on its RTBF obligations.[10] I had the opportunity to listen to and speak with many of Europe's leading thinkers on Data Protection. I highlight that background here in the interest of transparency. But I

[10] Advisory Council to Google on the Right to Be Forgotten, GOOGLE, https://www.google.com/advisorycouncil/.

also believe it gives me important perspective on the disconnect between well-meaning people on all sides of this issue, in particular between Data Protection and Intermediary Liability specialists. I will try to bridge that divide here.[11]

B. Using this Article as a Toolkit

This article tackles big questions. What is the proper role for private platforms in resolving conflicts between Internet users' privacy and information rights? If private companies must resolve such disputes, how can lawmakers promote fair outcomes? What do we do when different countries reach different answers to these questions?

To suggest answers to these questions, I will plumb the depths of two rather technical areas of law: Data Protection and Intermediary Liability. If you enjoy these fields and have time, I hope you will read the whole Article. But the Article is also drafted for maximum practical value to the busy people who will have the power and opportunity to solve the impending problems with RTBF under the GDPR. If you are an advocate, thinker, regulator, litigator, or anyone else confronting isolated facets of the issue, individual sections of the Article may give you analysis you can use. The Table of Contents is detailed and can lead you directly to specific topics. I hope that you will find analysis you can use to promote balanced protections for both privacy and free expression rights online.

The roadmap is this: Beginning in Section II, I will briefly review the history of Data Protection and Intermediary Liability law, their convergence in the RTBF, and the emergence of the EU's momentous new law, the GDPR. Section III will detail the new GDPR provisions that affect publicly shared online information and expression. It includes a careful overview of the law's problematic notice-and-takedown procedural

[11] I'm tremendously grateful to the people who lent their time and expertise to strengthen the article, including John Bowman, Neal Cohen, David Erdos, Peter Fleischer, Al Gidari, Jennifer Granick, Jim Greer, Joris van Hoboken, Chris Kuner, Harjinder Obhi, Miquel Peguera, and, Michel José Reymond. Mistakes are my own.

rules. Section IV will suggest a way to avoid those rules entirely, by invoking the EU's primary Intermediary Liability law, the eCommerce Directive, along with European courts' rulings connecting that law to fundamental rights.[12] Applying the eCommerce Directive in the Data Protection context would require the resolution of longstanding, but not insoluble, doctrinal disputes.

Each problematic provision of the GDPR comes with an opportunity to advance better interpretations. The law's ambiguity is in this sense an asset, an opening to seek better and more balanced readings. In Section V of the Article, I will list stand-out opportunities to do so. Specifically, I recommend:

1. Relying on rules based on the eCommerce Directive and fundamental rights considerations, rather than the GDPR, to govern notice-and-takedown procedures.

2. Interpreting individual GDPR provisions to mitigate the threats they pose to Internet users' rights, including both expression and privacy rights.

3. Limiting RTBF obligations to search engines such as Google or Bing, and not extending them to hosting platforms, such as Twitter or DailyMotion.

4. Encouraging OSPs to protect their users' expression, information, and privacy rights in response to RTBF requests by guaranteeing that the OSPs will not face financial penalties for doing so.

5. Adopting stronger express protections for information and expression rights.

6. Only requiring OSPs to honor RTBF requests in countries where doing so is consistent with national law.

In sum, European policymakers can protect online privacy and Data Protection rights, using existing European legal tools, without unnecessarily harming information and expression rights in the process. This Article will show how.

---

[12] Council Directive 2000/31/EC, European Parliament, 2000 O. J. (L178) 1 (hereinafter *EU eCommerce Directive*).

II. Convergence of Legal Frameworks

The law of Data Protection and the law of Intermediary Liability have been on a collision course for a long time, but cases squarely raising the two issues have emerged only recently. Historically, few lawyers needed to draw a connection between the two fields. They evolved differently. They use two distinct vocabularies, and are for the most part interpreted, enforced and litigated by different practitioners. A lawyer who views an issue through the lens of Intermediary Liability and one who views the same issue through the lens of Data Protection may have trouble even understanding each other's concerns.

In this Section of the Article, I will review the history of the two fields and their eventual convergence, first in *Google Spain* and now in the GDPR.

A. Intermediary Liability History and Law

The law of Intermediary Liability limits OSPs' legal responsibility for user activities, often by establishing notice-and-takedown obligations. By doing so, it protects individual Internet users' rights to seek and impart information. OSPs' liability protections or "safe harbors" reduce incentives they would otherwise have to build only "walled garden" platforms that exclude the general public, or to over-police and remove controversial but legal expression.

Intermediary Liability law sits at a unique and often troubling intersection of state and private power. When OSPs remove user expression based on actual or perceived legal requirements, the harm to the user's rights can be traced to state action. Removals motivated by fear of liability are in this sense different from the ones many OSPs carry out based on their own community guidelines or terms of service.[13] Voluntary content

[13] State action can of course also affect OSPs' nominally voluntary removal decisions. When it does, state human rights obligations may be implicated. This important issue is beyond the scope of this Article. *See generally* Backpage.com, LLC v. Dart, 807 F. 3d 229 (7th Cir. 2015) (sheriff violated U.S. First Amendment by pressuring credit card companies to terminate service to website based on the website's offensive but lawful activity); Recommendation 14, Council of Europe Commissioner for Human Rights,

removals also affect online expression, and are rightly scrutinized by Internet rights advocates. But they typically do not raise the specter, key to Intermediary Liability law, of "collateral censorship" based on state action. As Yale Law Professor Jack Balkin explains,

> Collateral censorship occurs when the state holds one private party A liable for the speech of another private party B, and A has the power to block, censor, or otherwise control access to B's speech. This will lead A to block B's speech or withdraw infrastructural support from B. In fact, because A's own speech is not involved, A has incentives to err on the side of caution and restrict even fully protected speech in order to avoid any chance of liability.[14]

Intermediary Liability protections allow private platforms to support public participation and expression at a scale never dreamed of pre-Internet. If YouTube had to review all 300 hours of video users upload each minute, for example, its operations would be impossible and the Internet would lose an important speech platform.[15]

Most Intermediary Liability systems immunize OSPs for standard technical operations but deny immunity for more active, conscious engagement -- if OSP's themselves author content, or assume practical responsibility for content posted by users, they may lose the

---

Prof. Douwe Korff, COUNCIL OF EUROPE, THE RULE OF LAW ON THE INTERNET AND IN THE WIDER DIGITAL WORLD 23 (2014), https://free-group.eu/2015/01/18/d-korff-the-rule-of-law-on-the-internet-and-in-the-wider-digital-world (states may have responsibility to limit even "measures implemented by private parties for business reasons, without direct involvement of the state"); Council of Europe, COMP. STUDY ON BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT: COMP. CONSIDERATIONS (2016), 786-87, http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet (summarizing arguments for liability of private OSPs for voluntary removals, or liability of governments for permitting such removals); CHRISTINA ANGELOPOULOS, ANNABEL BRODY, WOUTER HINS, BERNT HUGENHOLTZ, PATRICK LEERSSEN, THOMAS MARGONI, TARLACH MCGONAGLE, OT VAN DAALEN & JORIS VAN HOBOKEN, *Study of fundamental rights limitations for online enforcement through self-regulation,* 50-51 (2016), http://www.ivir.nl/publicaties/download/1796.

[14] Jack Balkin, *Old School/New School Speech Regulation*, 127 HARV. L. REV. 2296 (2014) at 2309. In unusual cases, economic incentives may weigh against removal. For ordinary user speech on large-scale platforms, however, liability risk is the biggest financial consideration. Minimizing such risk could even be seen as a fiduciary duty to shareholders.

[15] *Statistics,* YOUTUBE, (2015), https://web.archive.org/web/20150305153210/https://www.youtube.com/yt/press/statistics.html.

immunity.[16] OSPs are also typically liable if they know or should have known about unlawful content and fail to act.[17] To preserve immunity, OSPs operate notice-and-takedown systems. For large companies, this may mean having a standardized intake form for notices, a legal team dedicated to handling them, and specialized tools to track and act upon them. Smaller companies may have simpler systems, or no system at all, and respond ad hoc to notices.[18]

Anecdotal evidence and academic studies show that OSPs receive many inaccurate or bad faith removal requests – and, too often, comply with them.[19] For example, scholars reviewing Google's US copyright-based removals in 2006 found that almost a third of requests raised questionable legal claims.[20] Most data and anecdotal evidence of over-removal comes from copyright removals under the US Digital Millennium Copyright Act (DMCA),[21] because of the significant volume of removals and relatively high degree of public transparency possible under that law.[22] Notorious examples include copyright

---

[16] *See, e.g.*, C-324/09, L'Oreal SA v. eBay International AG, 2011 EUR-Lex CELEX No. 609CJ0324 at Rul. para. 6 (online marketplace may lose immunity under EU eCommerce Directive where it actively optimizes or promotes particular offers of sale); Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 40 (2nd Cir. 2012) (OSP might lose immunity for manually selecting user-generated videos for syndication to a third party).

[17] EU eCommerce Directive, Art. 14.1(a) (knowledge-based liabilities for hosts in the EU); 17 USC § 512(c)(1)(A) (knowledge-based liability for copyright claims against hosts in US); *but see* 47 U.S.C. § 230 (1996) (OSP complete immunity for non-intellectual property civil claims).

[18] *See* Jennifer M. Urban et al., Notice and Takedown in Everyday Practice, (March 29, 2016) UC Berkeley Public Law Research Paper No. 2755628 (2016) (unpublished paper), https://ssrn.com/abstract=2755628.

[19] Daniel Seng, *The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices*, 18 VA. J. L. & TECH. 369 (2014); Urban et al, *supra* note 18; Jennifer Urban and Laura Quilter, *Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMP. HIGH TECH. L. J., 621 (2005); Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet 2011*, CTR. FOR INTERNET & SOC'Y, http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf; Christian Ahlert, et al., *How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation*, CTR. FOR SOCIO-LEGAL STUD.: PROG. IN COMP.MEDIA L. & POL'Y, http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf; John Leyden, *How to Kill a Website with One Email: Exploiting the European E-Commerce Directive*, THE REGISTER, (Oct. 14, 2004), http://www.theregister.co.uk/2004/10/14/isp_takedown_study/.

[20] Urban and Quilter, *supra* note 19.

[21] 17 U.S.C. § 512 (1998).

[22] *See* LUMEN DATABASE, https://lumendatabase.org (Jan. 29, 2017).

claims attempting to remove consumer reviews,[23] Wikipedia articles,[24] major news sources,[25] and content licensed by the accuser.[26] Abusive DMCA requests have also been used to silence scientific[27] and religious[28] disagreement. According to transparency reports in 2015, Twitter rejects about 29% of DMCA removal requests as invalid;[29] Tumblr rejects about 15%;[30] and Automattic/WordPress rejects 45%.[31]

Practitioners, scholars, and NGOs have over time developed expertise about how to protect online expression against over-removal, by imposing checks and balances on the removal process. The Manila Principles, a set of notice-and-takedown rules endorsed by many Internet civil liberties organizations,[32] recommends:

- Requiring claimants to include adequate information in removal requests.[33]

---

[23] Eric Goldman, *The Latest Insidious Tactic To Scrub Online Consumer Reviews*, FORBES (July 23, 2013, 12:07 PM), http://www.forbes.com/sites/ericgoldman/2013/07/23/the-latest-insidious-tactic-to-scrub-online-consumer-reviews/#70cb4b6d7dde.

[24] Aaron Soupporis, *Microsoft Mistakenly Asks Google to Block the BBC, Wikipedia, US Government Webpages*, THE VERGE (Oct. 8, 2012, 7:50 AM), http://www.theverge.com/2012/10/8/3472662/microsoft-dmca-takedown-bbc-wikipedia-government-google-search.

[25] *Id*.

[26] Zahavah Levine, YouTube, *Broadcast Yourself*, YOUTUBE BLOG (Mar. 18, 2010), https://youtube.googleblog.com/2010/03/broadcast-yourself.html.

[27] Ivan Oransky, *WordPress Removes Anil Potti Posts from Retraction Watch in Error After False DMCA Copyright Claim*, RETRACTION WATCH (Feb. 5, 2014), http://retractionwatch.com/2013/02/05/wordpress-removes-anil-potti-posts-from-retraction-watch-in-error-after-false-dmca-copyright-claim/; John Timmer, *Site plagiarizes blog posts, then files DMCA takedown on originals*, ARS TECHNICA (Feb. 5 2013, 3:33 PM), http://arstechnica.com/science/2013/02/site-plagiarizes-blog-posts-then-files-dmca-takedown-on-originals/.

[28] Eva Galperin, *Massive Takedown of Anti-Scientology Videos on YouTube*, ELECTRONIC FRONTIER FOUND. (Sept. 5, 2008), https://www.eff.org/deeplinks/2008/09/massive-takedown-anti-scientology-videos-youtube.

[29] *Copyright Notice*, TWITTER, https://transparency.twitter.com/copyright-notices/2015/jul-dec.

[30] *Copyright and Trademark Transparency Report (Jan.-June 2015)*, TUMBLR., http://static.tumblr.com/zyubucd/0uWntp2iw/iptransparencyreport2015a_updatedfinal.pdf.

[31] *Intellectual Property: Copyright Report*, AUTOMATTIC/WORDPRESS, https://transparency.automattic.com/intellectual-property/2015-h2/

[32] *See* Manila Principles on Intermediary Liability, MANILAPRINCIPLES.ORG, https://www.manilaprinciples.org/ (hereinafter *Manila Principles*). Other model rules or guidelines from individual civil liberties organizations are listed *infra* note 49.

[33] *Id.* at 3.b; *see also* 17 U.S.C. § 512(c)(3)(A).

- Providing notice to the user whose content is alleged to violate the claimant' rights.[34]
- Giving the accused user the opportunity to contest the accusation.[35]
- Assessing fines, penalties or damages for removal requests made in bad faith.[36]
- Providing public transparency about removals.[37]
- Ensuring that OSPs are not forced to actively monitor or police user content.[38]

Procedural rules like these protect rights that in the US are listed in the Constitution, and in the EU are guaranteed under the Charter of Fundamental Rights of the European Union (Charter).[39] Following European parlance, I will refer to these as "fundamental" rights. Rights recognized in the EU that are affected by Intermediary Liability laws include free expression and information access;[40] privacy and Data Protection;[41] rights to conduct business and provide services;[42] rights to assembly and association,[43] and rights to effective remedies and fair trials.[44]

---

[34] *See Manila Principles*, *supra* note 32, at 5.

[35] *Id.*

[36] *Id.* at 3.g.

[37] *Id.* at 6. *See generally* Brief of Amici Curiae Chilling Effects Clearinghouse Leaders in Support of Appellee, Perfect 10, Inc. v. Google Inc., 2010 WL 5813411. (listing research and scholarship that depends on Lumen database (formerly known as Chilling Effects)).

[38] Manila Principles, *supra* note 32, at 1.d.

[39] Charter of Fundamental Rights of the European Union, 2012 O.J. (C326) 2; Angelopoulos et al., *supra* note 13.

[40] Charter, *supra* note 39, Art. 11, *see* C-360/10, SABAM v. Netlog NV, (2012) 2 C.M.L.R. 18 at para. 48 (citing as right threatened by OSP monitoring requirement).

[41] Charter, *supra* note 39, Arts. 7 & 8, *see* Netlog, (2012) 2 C.M.L.R. para. 46 (citing Data Protection as rights threatened by OSP monitoring requirement).

[42] Charter, *supra* note 39, Art. 16, *see* Netlog, (2012) 2 C.M.L.R. para. 46 (citing as right threatened by OSP monitoring requirement).

[43] Charter, *supra* note 39, Art. 12. *See* Angelopoulos et al., *supra* note 13, at 22 (discussing assembly right).

[44] Charter, *supra* note 39, Art. 47. *See* Angelopoulos et al., *supra* note 13, at 22 (discussing remedies rights); Martin Husovec, *Injunctions Against Innocent Third Parties: The Case of Website Blocking*, MAX PLANCK INST. INTELL. PROP. & COMPETITION L. RES. PAPER NO. 13-14 at 123 (2013) (discussing impact of ISP site-blocking on website operators under analogous fair trial right of European Convention on Human Rights).

The core Intermediary Liability law in the EU is the eCommerce Directive, enacted in 2000.[45] This EU-wide law functions roughly like a treaty, setting shared rules to be implemented in the national laws of Member States. It requires each Member State to provide special immunities for ISPs, hosts, and caching providers; legislators or courts in some countries have applied it to search engines as well.[46] The eCommerce Directive permits and encourages Member States to adopt specific procedures for notice-and-takedown.[47] A few EU countries have used this opportunity to establish detailed protections like those listed above. For example, Finnish law requires copyright holders to provide specified information before OSPs consider a removal request, and requires OSPs to give the alleged infringers notice and an opportunity to "counter-notice" or object to removals.[48] In 2012, a European Commission study found similar laws in five other countries.[49]

Many other EU countries have not legislated meaningful notice-and-takedown procedures, leaving an unfortunate degree of uncertainty about the rights and obligations of both Internet users and OSPs.[50] Even so, the eCommerce Directive itself provides

---

[45] EU eCommerce Directive, Art. 12-15.

[46] *See, e.g.*, Spain's Info. Soc'y Serv. and Elec. Com. L., Art. 17 (2002) http://www.boe.es/buscar/act.php?*id*=BOE-A-2002-13758, *discussed in* Peguera, *supra* note 3. *See also* SAIF v. Google France, Cour d'Appel [Paris] [Chambre 1], Jan. 26 2011, 08/13423, http://juriscom.net/wp-content/documents/caparis20110126.pdf (finding safe harbors for Google's image search under French law); *Mosley v. Google*, [2015] EWHC (QB) 59 [30] (holding that eCommerce Directive Art. 13 "applies to internet service providers such as Google who operate a search engine"); Joris van Hoboken, *Legal Space for Innovative Ordering: On the Need to Update Selection Intermediary Liability in the EU*, 13 INT. J. COMM. L. & POL'Y (2009) (detailing the position of search engines under the Ecommerce Directive).

[47] EU eCommerce Directive R. 46.

[48] Tuomas Mylle and Ulla-Maija Mylly, *Finland Country Report*, *Council of Europe Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content* (2016) at 221-222 and fn1 at 221, http://www.coe.int/en/web/freedom-expression/country-reports.

[49] *Commission Staff Working Document, e-Commerce action plan 2012-2015,* EUROPEAN COMMISSION (2012), http://ec.europa.eu/internal_market/e-commerce/docs/communications/130423_report-ecommerce-action-plan_en.pdf at 44 (procedures in Finland, Hungary, Lithuania, Spain and UK include "an obligation for intermediaries to offer a possibility to submit a counter-notice.") Even in legal systems that lack formal rules on point, the publisher's defenses may be relevant to the "knowledge" that triggers liability for the OSP.

[50] The European Commission has now twice officially considered overhauling the notice-and-action rules for OSPs operating under the EU eCommerce Directive. *See Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce*

important baseline rules. First, it establishes a "knowledge" standard for OSP liability: OSPs are immune until they have "knowledge of illegal activity or information" posted by users.[51] As the CJEU has noted, mere allegations may not meet this standard if they are "insufficiently precise or inadequately substantiated."[52] This standard makes it easier for OSPs to protect users' rights in the face of vague or unsubstantiated removal demands. In a few cases, courts have even held that mere allegations cannot establish OSP knowledge in difficult-to-resolve cases, and that claimants must instead prove their claims to an independent authority.[53] A Spanish appellate ruling provided perhaps the strongest statement of this standard, saying that OSPs should not remove user content without a court order or "set themselves up as judges of such content, since the aim is precisely to enhance freedom of expression online."[54]

(2000/31/EC), http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm; (2010) *Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy*, (2015) https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud. Public interest groups have issued detailed critiques and suggestions for improvement. *See, e.g.*, *Internet Intermediaries: Dilemma of Liability,* ARTICLE 19 (2013), https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf; *Response to EU Consultation on E-Commerce Directive*, EUROPEAN DIGITAL RIGHTS (EDRI) (2010), https://edri.org/files/EDRi_ecommerceresponse_101105.pdf; *LQDN's Draft Answer to the e-Commerce Consultation, LQDN* (2010), https://lqdn.co-ment.com/text/KALAphGyXcx/view/.

[51] EU eCommerce Directive Art. 14 (creating both actual and constructive knowledge standards for Internet hosts).

[52] L'Oréal, 609CJ0324 at para. 122.

[53] Royo v. Google (Barcelona appellate court judgment 76/2013 of 13 February 2013) (requiring court order unless validity of removal claim is manifest), *but cf.* Asociación de Internautas v. SGAE, 773/2009, (Supreme Court, Civil Chamber, December 9, 2009) (Spain's implementation of eCommerce Directive cannot require court orders for *every* removal); *see also* Davison v. Habeeb ([2011] EWHC 3031 (QB) para. 68 (notice of allegedly defamatory blog post did not create actual or constructive knowledge under eCommerce Directive where OSP was "faced with conflicting claims … between which it was in no position to adjudicate"). Two earlier UK cases discuss the issue of OSP "knowledge" under the eCommerce Directive, noting that "in order to be able to characterise something as 'unlawful' a person would need to know something of the strength or weakness of available defences." Bunt v. Tilley ([2006] EWHC 407 (QB)) (Mr. J. Eady) para 72, quoted in Kaschke v. Gray ([2010] EWHC 690 (QB)), *but see* Tamiz v. Google Inc. ([2013] EWCA Civ 68) (blogging platform can be liable as publisher of user content under defamation law, without consideration of eCommerce hosting defenses or standard for knowledge thereunder). *See also* Alberto Aranovitz, Portugal Country Report, Council of Europe Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet content (2016) at 544 http://www.coe.int/en/web/freedom-expression/country-reports (under Portuguese law, OSPs "not obliged to remove the content or to disable access to it merely because an interested party alleges that there has been a violation of the law," but must remove only "obviously illegal" content).

[54] Royo, supra note 53, Section 7 (informal translation).

A second key provision of the eCommerce Directive says that OSPs may not, under law, be given any "general obligation to monitor" or police users' online expression.[55] The ECHR and CJEU both have recognized that this rule protects fundamental rights of Internet users, in large part because monitoring requirements would foreseeably lead to over-cautious erroneous removal of lawful speech, and fewer open platforms for online participation.[56] ECHR case law rejecting over-reaching monitoring obligations rests on fundamental rights grounds alone, leading some scholars to suggest that the prohibitions in the eCommerce Directive may be "merely an explicit confirmation … of a limitation that would apply anyway as a result of constitutional considerations[.]"[57]

Intermediary Liability law under the eCommerce Directive is far from perfect. It typically lacks detailed procedural rules, and the protections created by the "knowledge" standard

---

[55] EU ecommerce Directive Art. 15.1 The exact parameters of the prohibited "general" monitoring obligation under EU law are disputed, and the issue is prominent in current Brussels policy discussions. *See* Monica Horten, *Content 'Responsibility': The Looming Cloud of Uncertainty for Internet Intermediaries*, CTR. DEMOCRACY & TECH. (Sept. 22, 2016) at 11, https://cdt.org/files/2016/09/2016-09-02-Content-Responsibility-FN1-w-pgenbs.pdf (listing 2016 policy initiatives including copyright, hate speech, and countering violent extremism initiatives with potential monitoring requirements for OSPs); Joe McNamee, *ENDitorial: What do two copywrongs make? Definitely not a copyright*, EDRI (Dec. 14, 2016) https://edri.org/enditorial-two-copywrongs-make-definitely-not-copyright/ (discussing monitoring provisions of proposed Copyright Directive); Daphne Keller, *Can a New Broadcasting Law in Europe Make Internet Hosts Monitor Their Users?* (May 27, 2016, 2:51 PM), http://cyberlaw.stanford.edu/blog/2016/05/can-new-broadcasting-law-europe-make-internet-hosts-monitor-their-users (discussing monitoring under proposed Audio-Visual Media Services Directive).

[56] *See* Magyar Tartalomszolgáltatók Egyesülete (MTE) v. Hungary (2016) E.Ct.H.R. 82, http://www.bailii.org/eu/cases/ECHR/2016/135.html (monitoring may not be mandated in case of defamatory speech in news forum comments); Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 2011 E.C.R. I-11959 para. 52); and SABAM v. Netlog, (2012) 2 C.M.L.R. at para. 48; *but see* Delfi AS v. Estonia (2015) E.Ct.H.R., http://www.bailii.org/eu/cases/ECHR/2015/586.html (monitoring requirement permissible in case of unprotected hate speech in news forum comments); *see generally* Daphne Keller, *New Intermediary Liability Cases from the European Court of Human Rights: What Will They Mean in the Real World?* (April 11 2016), http://cyberlaw.stanford.edu/blog/2016/04/new-intermediary-liability-cases-european-court-human-rights-what-will-they-mean-real. Courts and lawmakers around the world have reached similar conclusions under their own Intermediary Liability laws. *See*, *e.g.*, Corte Suprema [Supreme Court of Argentina], Civil, 29/10/2014,"Rodriguez M. Belen c. Google", R.522.XLIX, (rejecting requirement for OSPs to proactively monitor user speech on grounds of information rights); Shreya Singhal v. Union of India, (2015) 12 SCC 73 (India) (based on free expression considerations, construing Notice and Takedown statute to mandate removal only based on court or other government order).

[57] Angelopoulos et al, *supra* note 13, at 28.

and restriction of mandatory monitoring have been undercut by some courts and lawmakers.[58] But it does create basic tools to limit over-removal under notice-and-takedown systems -- in striking contrast to the GDPR, as we shall see.

The eCommerce Directive applies to all or nearly all legal removal claims received by OSPs, ranging from copyright to hate speech.[59] The one potential exception is for the claims discussed in this article – the ones based on Data Protection law.[60] This had little significance before the rise of the RTBF, because Data Protection law was not widely used as a ground for removing online content. Now, however, excluding these claims from the eCommerce Directive notice-and-takedown framework may have real consequences, depriving Internet users of procedural protections against over-removal.

B. Data Protection History and Law

The law of Data Protection is generally very foreign to US lawyers, but better known in much of the world. Versions of it exist in over a hundred countries,[61] often modeled on Europe's 1995 Data Protection Directive ("1995 Directive").[62]

---

[58] *See, e.g.*, Rome Court of Appeal, 20 april 2016, Reti Televisive Italiane S.p.A. (RTI) v. Break Media, 27 April 2016 (ad-supported video host ineligible for immunity). Horten, *supra* note 55 (discussing legislative threats to EU eCommerce Directive).

[59] *See,* Opinion of Advocate General Szpunar, Case C 484/14, Tobias Mc Fadden v. Sony Music Entm't Ger. ¶ 64 (Eur. Ct. Justice 16 Mar. 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1486427195652&uri=CELEX:62014CC0484) (citing proposal for a directive COM(1998) 586 final, p. 27) (immunity extends to "all forms of liability for unlawful acts of any kind, and thus to liability under criminal law, administrative law and civil law").

[60] *See* discussion *infra* Section IV.

[61] Graham Greenleaf, *Global Tables of Data Privacy Laws and Bills*, 133 PRIVACY L. & BUS. INT. REP., 18-28, (2015) (listing 109 countries).

[62] Council Directive 95/46/EC, European Parliament, 1995 O. J. (L 281) 31 (hereinafter *1995 Directive*); *see generally* Paul M. Schwartz and Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877 (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2271442 (comparing US and EU approaches); James Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004) (same).

In the EU, Data Protection is a fundamental right, distinct from the right to privacy.[63] It emerged from 20th century concerns about large scale records and databases tracking information about citizens, and serves to protect an individual's sphere of "informational autonomy" against such activity.[64] Data Protection claims can extend to any information relating to oneself, not just information that is intimate, embarrassing, or offensive. It provides legal rights against acts, like an employer's ongoing storage of outdated employee files, for which courts might not recognize a privacy claim. When the right to Data Protection conflicts with other fundamental rights, including rights to receive and impart information, lawmakers must balance the rights.[65]

The 1995 Directive sets out a detailed framework for Data Protection, and establishes regulatory bodies for enforcement. National and sub-national Data Protection Authorities (DPAs) are the primary enforcers, and have ongoing relationships with many regulated companies. The Article 29 Working Party, an influential regulatory organization established under the Directive, issues highly influential – though non-binding – interpretations of Data Protection law.[66]

Data Protection law governs the "processing" of "personal data." Both terms are defined very broadly. Personal data includes "any information relating to an identified or identifiable natural person[.]"[67] "Processing" is

---

[63] Charter Art. 8.

[64] *See, e.g.*, Viktor Mayer-Schönberger & Yann Padova, *Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation*, 17 COLUM. SCI. & TECH. L. REV. 315, 332 (2016); Paul Schwartz, *Privacy And Participation: Personal Information And Public Sector Regulation In The United States*, 80 IOWA L. REV. 553, 562 (1995).

[65] *See, e.g.*, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, EUR-Lex CELEX No. 606CJ0275, (Jan. 29, 2008); C-314/12, UPC Telekabel v. Constantin Film, EUR-Lex CELEX No. 62012CJ0314.

[66] 1995 Directive Art. 29.1 (noting "advisory status"). *See also* Opinions and Recommendations: Article 29 Working Party, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

[67] 1995 Directive Art. 2.a.

> any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[68]

These definitions bring a remarkable array of activities and information within the ambit of Data Protection law – from online restaurant orders to historical archives to privately operated websites.[69]

Entities may process personal data only if they meet one of six listed legal justifications -- for example, if they have the consent of the data subject or are legally obliged to process the data.[70] A catch-all category permits processing "necessary for … legitimate interests."[71] As will be discussed below, this "legitimate interests" criterion is key for OSP operations under both the 1995 Directive and the new GDPR.

For entities subject to Data Protection law, a key distinction is whether the law classifies them as "Controllers" or "Processors." Distinct legal obligations flow from each classification. Controllers are, roughly speaking, entities that hold personal data and decide what to do with it.[72] Because they are the decision-makers, they have far more obligations under the law. Importantly for this Article, this includes compliance with erasure or RTBF requirements.

---

[68] 1995 Directive Art. 2.b.

[69] Case C-101/01, Bodil Lindqvist v Åklagarkammaren i Jönköping, 2003 E.C.R. I-04989) (defendant violated Data Protection law by operating a website for her church listing volunteers' names, telephone numbers, hobbies, and in one case "sensitive" medical information about a recent injury).

[70] 1995 Directive Art. 7, 9, 13 The Directive effectively authorizes some other uses of data that are not listed in this section through other exemptions or derogations, such as those covering journalism.

[71] 1995 Directive Art. 7(f).

[72] Under Article 2(d) of the 1995 Directive, "'Controller' shall mean the natural or legal person…which alone or jointly with others determines the purposes and means of the processing of personal data[.]"

Processors hold personal data, but follow instructions from a Controller about what to do with it.[73] 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 by instructing a payroll company, that company is a Processor.

The person whose personal data is being processed is called the "data subject." The Directive enumerates her rights, including compelling Controllers to erase data about her.[74]

This framework emerged from an era when data processing was largely a matter for banks, employers, sports clubs, doctors, and other brick-and-mortar entities. As will be discussed below, the expansion of Internet technologies created significant difficulties in mapping the Data Protection framework onto unanticipated and complex technologies.

C. Data Protection and Online Service Providers

OSPs are complex creatures under Data Protection law. In one respect, as operators of proprietary back-end databases and storage systems containing records of users' clicks, purchases, and other online behavior, they look like classic Data Controllers. At the same time, OSPs process "data" in the form of content created and shared by their users. A user who posts a group photo or a comment about another person is putting *that* data subject's personal data in the hands of an OSP. Identifying the OSP's duties to both the speaker and the person being spoken about, and fitting online speech into a traditional Data Protection legal framework, is difficult.

---

[73] *See Id.* at 2(e) ("'Processor' shall mean a natural or legal person … which processes personal data on behalf of the Controller"). *See also* Article 29 Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (2010), EUROPEAN COMMISSION, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

[74] 1995 Directive Art.12(b).

Suppose I tweet, "Matilda Humperdink served bad fish at her party last night. We all got sick - even Matilda!" By posting this, I act as Controller of the information about Matilda – including the "sensitive" information about her health, which typically may not be processed without her consent.[75] Does Twitter become a Controller of that information as well? Can she oblige Twitter to delete my post?[76] If Google indexes the tweet, what obligations does it have? Should the answers to these questions change if Matilda is the CEO of a corporate restaurant chain, and the party was one of her restaurant openings? Because Data Protection law has historically applied to back-end processing such as stored hospital records or Internet user logs, it has rarely needed the doctrinal tools to answer questions like these about public information and speech.[77]

The expression posted by users on OSP platforms is a form of data, but it is very different from the back-end files, logs, or profiles typically governed by Data Protection law. The difference between public expression and back-end data is very important. The two differ not only as a technical matter, but as a matter of fundamental rights.

When an Internet company generates back-end data by tracking user activity, only two sets of rights are generally affected: those of the user, and those of the company. Giving the user a simple, streamlined process to enforce Data Protection rights against the company makes sense.

---

[75] 1995 Directive Art. 8; Article 29 Working Party, *Opinion 5/2009 on online social networking (EC)* (June 12, 2009), 01189/09/EN (WP 163) at 8, (hereinafter *Article 29 Social Networks Opinion)* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

[76] The removal question becomes simpler when fewer parties are involved. As a data subject, I would generally be entitled to remove my own tweet. And if Matilda asked me to delete the tweet, instead of asking Twitter, I would have to assess my own duties as Controller (potentially jointly with Twitter) of the data in the tweet. *See generally* Brendan van Alsenoy, *The Evolving Role of the Individual Under EU Data Protection Law* 22-24 (CiTiP Working Paper 23/2015, 2015).

[77] Many possible tensions with Data Protection law and free expression are alleviated by exceptions in the law for journalism, resulting in a body of law tailored to that context, and generally less helpful for ordinary Internet users. David Erdos, *Beyond 'Having a Domestic'? Regulatory Interpretation of European Data Protection Law and Individual Publication* (forthcoming 2017) (manuscript on file with author).

For public expression, like my tweet about Matilda Humperdink, the situation is very different. A request to erase this data affects at least four key sets of rights: my rights to free expression, Matilda's rights to Data Protection and privacy, other Internet users' rights to seek and access information, and Twitter's rights as a business.[78] Rules that make sense for the simpler two-party situation will not work well to protect all of these conflicting interests. Adding expression and information rights to the mix makes both substantive and procedural barriers to improper data erasure much more important.

Data Protection experts recognized and wrestled with these issues as Internet platforms matured in the late 2000s. The Article 29 Working Party issued opinions about both social media[79] and search engines.[80] While these were to some extent superseded by subsequent developments – including *Google Spain* – they are good windows into the difficulty of fitting OSPs into the Data Protection framework.

In the social media opinion, the Working Party concluded that social media platforms are Controllers. The opinion did not probe the differences between back-end data and user-generated expression, but its discussion included both.[81] If correct, this classification leads to strange results. For example, per the Working Party's opinion, as a Controller, a social network could only process information about Matilda Humperdink's health status

---

[78] A complete list would include Twitter's own expression and information rights and other rights discussed *infra* Section III.A.

[79] *See Article 29 Social Networks Opinion*, *supra* note 75*;* Article 29 Working Party, *Opinion 1/2010 on the Concepts of "Controller" and "Processor" (EC)* (Feb. 16, 2010), 00264/10/EN (WP 169) (hereinafter *Article 29 Controller/Processor Opinion*), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. In the more recent opinion, the Working Party suggested that social networks and their users are both Controllers with respect to information posted by the user (p. 21, example 12), while a telecommunications operator offering bare-bones email services is to "be considered Controller only for traffic and billing data, and not for any data being transmitted" in the e-mail (p. 11, example 1).

[80] Article 29 Working Party, *Opinion 1/2008 on Data Protection Issues Related to Search Engines (EC),* (Apr. 4, 2008), 00737/EN (WP 148), at 23 (hereinafter *Article 29 Search Engine Opinion)*, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf.

[81] *Article 29 Social Networks Opinion, supra* note 75. The scant case law to date is discussed *infra* Section III.B. *See also* Natali Helberger and Joris van Hoboken, *Little Brother is Tagging You - Legal and Policy Implications of Amateur Data Controllers*, 4 Computer Law International (CRi), 101-109 (2010); Erdos *supra* note 77; van Alsenoy, *supra* note 76.

with her consent, or if she herself publicized the data.[82] That would put Twitter in breach of the law from the moment I tweeted. Social media platforms must also, the opinion said, let people access, correct or delete information posted about them – seemingly even in closed groups or private messages.[83]

The search engine opinion is more thoughtful regarding the distinction between back-end "user data" and what it calls "content data" – expression and information from third party webmasters, which Google indexes.[84] For "content data," it says, "search engine providers are generally not to be held primarily responsible under European Data Protection law."[85] Thus a search engine

> should not be considered to be the principal Controller with regard to the content…. The formal, legal and practical control the search engine has over the personal data involved is usually limited to the possibility of removing data from its servers.[86]

This distinction, though helpful, still does not fully reconcile search engine or other OSPs' operations with EU Data Protection requirements. For one thing, OSPs' legal justification for processing "content data" in the first place is the 1995 Directive's catch-all provision for "legitimate interests."[87] This vague "legitimate interests" concept is a slim reed upon which to rest the entire edifice of OSP operations. It is legally insufficient for processing health status and other sensitive personal data. As a result, as Professor

---

[82] *Article 29 Social Networks Opinion, supra* note 75, at 8. They may not seek her consent, however, unless she is already a platform member. *Id.* ("a possible e-mail invitation to join the SNS in order to access these personal data would violate the prohibition laid down in Article 13.4 of the ePrivacy Directive").

[83] *Id*. at 11. The Social Networks Opinion also prohibits social networks from retaining information about the reasons a user's account was terminated, and allows them to retain information identifying those accounts for only a year. *Id.* at 10. This is difficult to reconcile with other standard operations of OSP hosts, including the repeat infringer policies of the US DMCA. 17 U.S.C. § 512.

[84] *Article 29 Search Engine Opinion, supra* note 80, at 24.

[85] *Id.* at 23.

[86] *Id*. at 14.

[87] 1995 Directive Art. 7(f). *See also* Article 29 Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales C-131/12 (EC)* 5, (Nov. 26, 2014) 14/EN (WP 225), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf (hereinafter Article 29 Google Spain Guidelines) ("The legal ground for [search engine] processing under the EU Directive is to be found in Article 7(f)[.]")

Miquel Peguera has noted, classifying search engines as Controllers would seemingly render them "incompatible with EU law" because they are "unable to comply with most of the obligations the Directive imposes on data controllers."[88]

D. The *Google Spain* Ruling

Mounting concerns about online Data Protection came to a head in the CJEU's *Google Spain* case. The case is explained in detail in numerous other sources, so this article will summarize it only briefly.[89]

The case concerned a Spanish man, Mario Costeja González, whose property was auctioned for non-payment of debts in 1998.[90] A Barcelona newspaper, *La Vanguardia*, published a legally mandated announcement of the auction, including Mr. Costeja's name.[91] Ten years later, the paper digitized its archives and made them available online.[92] People using Google to search for Mr. Costeja's name could find the notice among the top results.[93] Mr. Costeja, who had since resolved his financial problems, complained to the Spanish DPA and obtained an order for Google to remove the results.[94]

Google appealed the order through the Spanish courts, which eventually referred key questions to the CJEU. At issue were a series of interlocking doctrinal questions, all of which needed to be resolved in Mr. Costeja's favor for him to prevail.[95] The answers to

---

[88] Peguera, *supra* note 3 at 539. As another example, Controllers generally must notify data subjects at the time of collecting data about them from third parties. 1995 Directive Art.11. For OSPs that "collect" users' posts, identifying and notifying any individual mentioned would be more than difficult. For this requirement, OSPs can invoke an exemption based on difficulty, but it is noteworthy that the central Data Protection concept of notice is so ill-suited to OSPs processing user-generated content.

[89] *See, e.g.,* Peguera, *supra* note 3, van Hoboken, *supra* note 3.

[90] *Google Spain*, *supra* note 2, at para. 14.

[91] Peguera, *supra* note 3 at 523.

[92] *Id.*

[93] *Id.*

[94] *Id.* at 523-24.

[95] These included detailed questions about jurisdiction and the applicability of the 1995 Directive to Google's American parent company Google Inc.; questions about data processing and whether Google

these questions were far from clear: the CJEU's own Advocate General – whose advice the Court typically follows – said the DPA's removal order was not valid.[96]

The Court, however, found in Mr. Costeja's favor. Critically, it concluded that Google acted as the Controller of the indexed auction announcement, because it determined the purposes and means by which it processed that content.[97] The Court focused on Google's indexing function, noting that web search engines aggregate disparate, previously unconnected information "to establish a more or less detailed profile of the data subject."[98] This processing, the court noted, was different than *La Vanguardia*'s, and subject to separate analysis and obligations under Data Protection law.[99] For this reason, a search engine could be obliged to remove links to information on webpages even "when its publication in itself on those pages is lawful."[100]

The Court said that, as a Controller, Google must honor erasure requests and objections to processing under the 1995 Directive.[101] It established what was effectively a notice-and-takedown process, without reference to Google's status as a protected intermediary under Spain's implementation of the eCommerce Directive.[102] Specifically, it must remove the specified links from the list of results that appear when users search for the

---

acted as a Controller for indexed data; and questions about the existence and scope of a 'right to be forgotten' under Articles 12 and 14. *See Google Spain*, *supra* note 2, at para. 20.

[96] The Advocate General, who functions somewhat like a prestigious, public clerk in recommending outcomes to the Court, concluded that Google in most cases does not act as a Controller. In any case, he said, the 1995 Directive did not create a right to "be forgotten" by deleting publically available information based on the data subject's personal preference. Opinion of Advocate General Jääskinen, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ¶ 20 (Eur. Ct. Justice, June 25, 2013), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN. *See generally* Carlos Arebola et al., *An Econometric Analysis of the Influence of the Advocate General on the Court of Justice of the European Union*, 5 CAMBRIDGE J. COMP. INT'L L., 1, (2016) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2714259.

[97] *Google Spain*, *supra* note 2, at Rul. para. 1, applying 1995 Directive Art. 2(d) definition of Controller.

[98] *Id.* at para. 33.

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

[100] *Id*. at para. 88.

[101] *Id*. at Rul. para. 3, citing 1995 Directive Art.12 and 14.

[102] Spain's Info. Soc'y Serv. and Elec. Comm. L., *supra* note 46.

data subject's name.[103] The same results could still appear in results for other search terms, however. For example, a page discussing Matilda Humperdink's food poisoning might still appear when people search for "fish," but not when they search for "Matilda Humperdink." Data from the page, usually including all its text, could also persist on Google's servers to power its search results.

The Court was less clear about how Google or other search engines should determine which removal requests to honor.[104] It instructed them to remove data that is inaccurate or "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing,"[105] even if the information is true[106] or causes no prejudice to the data subject.[107]

RTBF requests are not to be honored, though when,

> the interference with [the requester's] 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.[108]

"[A]s a rule" however, the public's interest in information does not outweigh the data subject's Data Protection interests.[109] The Court did not identify or discuss the free

---

[103] *Google Spain*, *supra* note 2, at para 82.

[104] Some object to the term "removal" to describe the de-listing required by *Google Spain*, because the data still appears in other search results. *See*, *e.g.,* Joe McNamee, Google's forgetful approach to the "right to be forgotten" EDRI (Dec. 14 2016), https://edri.org/googles-forgetful-approach-right-forgotten/. I use it in this Article to refer both to search indexes de-listing information and hosts deleting it. This broad sense of the word, encompassing both complete and partial deletion, has long been conventional in the Intermediary Liability context. *See, e.g.*, *URL removals explained, part II: Removing sensitive text from a page,* GOOGLE (Aug. 6 2010), https://webmasters.googleblog.com/2010/04/url-removals-explained-part-ii-removing.html (describing process to "remove the snippet and the cached page" while leaving the rest of a search result intact); Mashable, *The countries where Facebook censors the most content* (Nov. 7 2014), http://mashable.com/2014/11/07/facebook-censorship-map/#eJe1oxpjGmq3 (describing content as "removed" when Facebook blocks some but not all users from seeing it based on national law).

[105] *Id.* at para. 92, 94 (paraphrasing 1995 Directive Article 6.1(c)).

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

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

[108] *Google Spain*, *supra* note 2, at para. 97.

[109] *Id.* at para 97.

expression rights of the website operator or publisher, or how exclusion from some Google search results could affect those rights.[110] This prioritization of Data Protection over other rights generated considerable controversy both in popular press and among legal experts.[111]

Since the ruling, Google and Microsoft have been asked to de-list some 1.8 million URLs, and have actually de-listed approximately 680,000.[112] Norms and standards, including thoughtful guidelines from the Article 29 Working Party, have begun to emerge to guide search engines in distinguishing valid from invalid RTBF requests.[113] Some cases in which Google declined to de-list have been brought to DPAs and national courts, creating a small but growing body of precedent.[114]

When Google *does* remove results, however, there is almost no analogous public review. Publishers do not have recourse to a regulatory agency to review their free expression claims, and may lack legal standing to challenge a removal in any case. Thus, courts and regulators have ample opportunity to enforce the status quo or to require more de-listing, but there is no good mechanism for them to move the needle in the other direction – toward de-listing less.

---

[110] *See* Peguera, *supra* note 3 at 555. The newspaper that published Mr. Costeja's information was not a party to the CJEU case, so no one before the court directly represented publishers' interests.

[111] *See, e.g.*, van Hoboken, *supra* note 3 (observing that Court's requirement of "effective and complete" protection for Data Protection rights is in tension with the broader need to balance Data Protection against other fundamental rights). Other important critiques of the ruling, including many rooted in Intermediary Liability concerns, are well summarized in *Ausloos and Kuczerawy*, *supra* note 3.

[112] Google Transparency Report, https://www.google.com/transparencyreport/removals/europeprivacy/; Microsoft Content Removal Requests Report, https://www.microsoft.com/about/csr/transparencyhub/crrr/.

[113] *Article 29 Google Spain Guidelines, supra* note 87; *see also* Advisory Council to Google on the Right to Be Forgotten, Final Report, GOOGLE, https://www.google.com/advisorycouncil/.

[114] *See, e.g.*, Stefan Kulk and Frederik Borgesius, *Freedom of expression and 'right to be forgotten' cases in the Netherlands after Google Spain*, 2015 EUR. DATA PROT. L. REV. 2, p. 113-125; Peguera, *No more right-to-be-forgotten for Mr. Costeja, says Spanish Data Protection Authority* (Oct. 3, 2015, 8:24 AM), http://cyberlaw.stanford.edu/blog/2015/10/no-more-right-be-forgotten-mr-costeja-says-spanish-data-protection-authority (following CJEU ruling, Spain's DPA rejects Mr. Costeja's removal request).

While some degree of consensus has emerged on the substantive criteria for RTBF removals, the same cannot be said for the procedure and technical implementation. In particular, disputes about jurisdiction have grown increasingly acute, with the French DPA maintaining that Google must remove search results globally, even in countries that do not recognize a RTBF.[115]

Data Protection authorities have also clashed with Google on questions about transparency for RTBF removals. They disputed Google's practice of routinely notifying webmasters when pages from their sites were removed from search results, arguing that the company should notify and consult with webmasters only in exceptional, difficult cases.[116] Some public debate also centered on Google's attempts to notify users when search results were modified in response to RTBF requests.[117]

Oceans of scholarly ink have been spilled discussing the *Google Spain* case and the questions it generated. The same cannot be said of the legislative provision that will soon take its place: the EU's sweeping new GDPR.

E. The 2016 General Data Protection Regulation

The GDPR is a comprehensive overhaul of EU Data Protection law, codifying new rules for RTBF and much more. As will be discussed throughout this Article, it introduces new

---

[115] Mark Scott, *Google Appeals French Privacy Ruling*, New York Times (May 19, 2016), http://www.nytimes.com/2016/05/20/technology/google-appeals-french-privacy-ruling.html?_r=0; *see also* D. Keller and B. Brown, *Europe's Web Privacy Rules: Bad for Google, Bad for Everyone*, NY TIMES (April 26, 2016), http://www.nytimes.com/2016/04/25/opinion/europes-web-privacy-rules-bad-for-google-bad-for-everyone.html?_r=1.

[116] *Article 29 Google Spain Guidelines*, *supra* note 87, at 10. More recently, Spain's DPA fined Google 150,000 Euros for notifying webmasters about a RTBF removal. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, RESOLUCIÓN: R/02232/2016, http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2016/common/pdfs/PS-00149-2016_Resolucion-de-fecha-14-09-2016_Art-ii-culo-10-16-LOPD.pdf.

[117] Notice about removals to people *seeking* content online is another important check on over-removal. Google tried to address this for the RTBF through near-ubiquitous notices on search results pages. These don't specify what content was removed, though, and Article 29 Working Party has said Google would violate the law if they did. *Article 29 Google Spain Guidelines*, *supra* note 87, at 3.

rules that are both harder to understand than those established by *Google Spain* and more dangerous to online information and expression.

The new Regulation replaces the 1995 Directive's scant 12,000 words with over 50,000 new ones, developed through multiple drafts and years of discussion.[118] Because it is a Regulation rather than a Directive, it will not have to be implemented as separate legislation in each EU country. It will go into effect across the EU in May of 2018.[119]

The GDPR makes sweeping changes to Data Protection law. For OSPs, many of the law's most important new terms are not about users' expression, but rather about the companies' own collection and use of back-end stored data about user behavior. Complying with those new rules may require engineering work to change logging and storage;[120] user interface redesign to introduce new notices and consent processes;[121] written Data Protection Impact Assessments;[122] extensive new internal record-keeping;[123] renegotiating contracts with other Controllers or Processors;[124] and in many cases appointing a data protection officer resident in the EU.[125] An influential guide for in-house lawyers concludes that, under the GDPR, "[d]ata protection will be as significant as antitrust or anti-corruption in terms of compliance risk," and is "likely to require

---

[118] *See*, *e.g.*, European Data Protection Supervisor, *EU Data Protection Reform*, EU, https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package; Opinions & Papers, WILSON SONSINI, https://www.wsgr.com/eudataregulation/opinions-papers.htm.

[119] GDPR Art. 91(2); European Commission, *Reform of European Data Protection Rules*, http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

[120] GDPR Art. 5 (Principles relating to processing of personal data), 25 (Data Protection by Design and Default).

[121] GDPR Art. 12-13 (new categories of information that must be included in privacy policies or similar notices); Art. 6(1)(a); 7; 9(1) & 9(2)(a), (conditions for consent to processing including user interface checkboxes); Hunton & Williams, *The Proposed EU General Data Protection Regulation: A Guide for In-House Lawyers* 23,28 (June 2015), https://www.huntonregulationtracker.com/.

[122] GDPR Art. 35.

[123] GDPR Art. 30.

[124] GDPR Art. 28-30.

[125] GDPR Art. 37-39.

organisation-wide changes for many businesses."[126] One set of researchers – funded by Google – predicted that small and medium enterprises would need to increase IT budgets by 16-40% to comply with the GDPR.[127]

The GDPR also stakes out expansive new extraterritorial application to companies outside of the EU.[128] And it arms regulators with the power to impose unprecedented fines: in principle, these could be as high as 4% of a company's annual global turnover or €20 million.[129] It also establishes a new European Data Protection Board ("the Board"), a successor organization to the Article 29 Working Party with broader powers and responsibilities.[130]

Significant questions remain about what the new law actually means. As I will discuss in Section III.C, it introduces ambiguous new language in some cases and in others reuses formulations from the 1995 Directive that have long been subject to disputed interpretations. This leaves considerable room for interpretation by regulators and courts.

Two sets of authorities will be particularly well positioned to proactively resolve questions about RTBF and information rights under the GDPR. The first is the Board, which is charged with issuing best practices guidelines for RTBF procedures.[131] The second is EU Member state legislatures, which are supposed to pass laws protecting free expression under the GDPR, and which have surprisingly broad additional powers to modify the Regulation's terms in their national law.[132] Litigation and court rulings, too,

---

[126] Hunton & Williams, *supra* note 121, at 6.

[127] L. Christensen *et al., The Impact of the Data Protection Regulation in the E.U.*, (Feb. 13, 2013), http://www.analysisgroup.com/uploadedfiles/content/insights/publishing/2013_data_protection_reg_in_eu_christensen_rafert_etal.pdf

[128] *See* discussion *infra* Section III.E.

[129] GDPR Art. 83.5(b).

[130] GDPR Art. 68 (establishing Board), 94.2 (references to A29 in existing law to be construed as references to Board).

[131] GDPR Art. 70.1(d).

[132] GDPR Art. 85, discussed *infra* Section III.D; William Long and Francesca Blythe, *Member States' derogations undermine the GDPR*, SIDLEY & AUSTIN: PRIVACY L. & BUS. UK REP. (May 2016),

will eventually shape understanding of the GDPR. But litigation is not a good avenue for mitigating risks posed by the GDPR, both because it would address issues only piecemeal and because of the practical situation of potential litigants: online publishers and speakers will have little opportunity to contest improper removal of their expression, and OSPs may be reluctant to do so on their behalf.

III. Threats to Information Rights Under the General Data Protection Regulation

This section reviews in detail the GDPR's rules governing RTBF requests, and identifies ways in which they tilt the playing field against online expression and information rights. An underlying problem with these GDPR provisions is their opacity. As Section III.A discusses, if OSPs do not understand what the law requires, the safe course will be to simply remove or de-list information.

Section III.B will consider whether RTBF requirements will apply to Internet hosts like Twitter or DailyMotion – a highly consequential question on which the GDPR is silent. The next Section, III.C, will walk through an OSP's process for notice-and-takedown under the GDPR. It will discuss how OSPs are likely to interpret the law's requirements in practice, as well as alternate interpretations that could be advanced to better protect online expression. Section III.D will review the law's free expression provisions, and identify important shortcomings. Finally, Section III.E, will discuss the law's extra-territorial application to information created and shared outside of the EU.

Cumulatively, these GDPR provisions make RTBF claims uniquely powerful legal tools– both for legitimate claimants and for abusive ones targeting information the public has a right to see.[133] A person asserting the RTBF can bypass long-standing substantive legal

---

http://www.sidley.com/publications/member-states-derogations-undermine-the-gdpr (discussing other Member State powers under GDPR).

[133] Given the unique power of RTBF claims, it is possible that in the future they could displace claims such as defmation, becoming the primary legal tool for individuals to control what others can say about them

defenses that would shield lawful speech against claims based on traditional reputational harms, such defamation or invasion of privacy.[134] As Professor Joris van Hoboken has pointed out, these well-established laws already address many of the problems covered by RTBF claims, and 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."[135]

The GDPR's notice-and-takedown rules also appear to provide RTBF claimants with great procedural advantages compared to other notice-and-takedown claimants, as Section III.C will detail. Later, in Section IV, I will propose a way to restore balance in this regard, by applying law under the EU's eCommerce Directive. That approach could preserve the GDPR's pro-privacy goals while avoiding many of the harms to online speech described here.

A. Unclear Rules and One-Sided Incentives

It is hard to read the GDPR, and that is a problem. Even Data Protection experts can't say for sure how the GDPR answers hugely consequential questions, like whether hosting platforms must carry out RTBF removals. It is even harder to parse the detailed provisions affecting notice-and-takedown operations. The Regulation's ambiguous requirements, coupled with its incentive structure for OSPs, will systematically push toward acceptance of over-reaching removal requests.

---

online. Claims brought by government, commercial, or other non-individual interests -- including most intellectual property claims -- would continue to rely on other laws.

[134] *See* Testimony of Gabrielle Guillemin, Article 19, Google Advisory Council on the Right to Be Forgotten (Oct. 16, 2014), https://docs.google.com/document/d/1kI269r0gW7lmvpe4ObRvRB_-68JN2yRSb-g2s3JD9qo/pub.

[135] Joris van Hoboken, *The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment* (2013) at 23, http://www.law.nyu.edu/sites/default/files/upload_documents/VanHoboken_RightTo%20Be%20Forgotten_Manuscript_2013.pdf.

It is generally accepted that the rule of law requires "the effect of legislation [to] be clear and predictable for those who are subject to it."[136] Where laws affect free expression rights under the European Convention, this predictability requirement is particularly stringent.[137] As the US Supreme Court has described the problem, unclear speech regulations may cause citizens "steer far wider of the unlawful zone… than if the boundaries of the forbidden were clearly marked."[138]

The risk that lawful speech will be suppressed through cautious overcompliance is increased when an OSP – rather than the speaker herself – decides how to interpret an unclear regulation. This concern about OSPs' over-compliance in blocking lawful information is sufficiently serious that, in a case involving an unclear judicial injunction, the CJEU required that Internet users be permitted to challenge overblocking in court.[139]

For each ambiguity in the GDPR, there are clear incentives for OSPs to err on the side of protecting the requester's Data Protection rights, rather than other Internet users' Expression rights. A brief review of the GDPR will tell companies that they face fines as high as to €20 million,[140] easily dwarfing the risk from most legal takedown demands, including the €137,000 ($150,000) potentially at stake for US DMCA copyright removals.[141]

---

[136] Joined cases 212 to 217/80 Amministrazione delle finanze dello Stato v Salumi [1981] ECR 2735, para 10; *see also* European Commission, *A New EU Framework to strengthen the Rule of Law (Annex)*, (Mar. 11, 2014), http://ec.europa.eu/justice/effective-justice/files/com_2014_158_annexes_en.pdf.

[137] *See* European Convention on Human Rights Art. 10.2, ETS 5 (restrictions on free expression violate fundamental rights unless "provided by law"); Ahmet Yildirim, App. No. 3111/10, E.Ct.H.R. ("provided by law" standard means "drafted with enough precision to enable any person, taking informed advice as needed, to regulate her / his behavior"). Some might argue that so long as RTBF involves only de-listing, rather than erasure, the law does not restrict speech and thus this standard does not apply.

[138] Baggett v. Bullitt, 377 U. S. 360, 372 (1964) (quoting Speiser v. Randall, 357 U. S. 513, (1958)).

[139] Telekabel, 62012CJ0314.

[140] GDPR Art. 83.5. The GDPR also provides for damages to the harmed data subject. GDPR Art. 82.

[141] 17 U.S.C. § 504. The largest Data Protection fine currently authorized in the UK is about €650,000 (£500,000) and the largest fine actually assessed is about €325,000 (£250,000). Hunton & Williams, *supra* note 121 at 12.

OSPs who contact DPAs or are able to obtain expert counsel will almost certainly be advised not to worry about fines of this magnitude. The GDPR requires that fines be "effective, proportionate, and dissuasive," and few expect regulators to punish Data Controllers that act in good faith.[142] But it is unrealistic to expect most OSPs to know this – particularly if they come within the GDPR's jurisdictional scope, but have no experience with EU law. A growing startup in India or Brazil with hopes of expanding into European markets, for example, has reason to avoid legal trouble there, and little ability to ascertain whether a RTBF request is legally valid.

For larger and more sophisticated OSPs, the sheer number of RTBF requests – each one posing a separate risk of penalties or damaged relationships with DPAs if the OSP fails to remove content – may create similar pressures. Incentives to overcomply may be reinforced by fear of attention from Data Protection regulators. Once a company is under review, it could be found noncompliant with the GDPR's other rules and subject to additional fines or even requirements to redesign its products.[143] Companies unsure of their status as Processors or Controllers may also hesitate to challenge RTBF claims, since being deemed Controllers would add significantly to their compliance obligations.

As a practical matter, Internet users' rights will be shaped not by the best or most accurate interpretation of the GDPR, but by the one companies actually adopt in the face of unclear rules, high potential penalties, and minimal transparency or public review. This practical backdrop will affect the real-world outcome of every legal ambiguity identified in this Article.

B. Right to Be Forgotten Obligations for Hosts and Social Media

One of the biggest open questions about the new RTBF provisions is whether they apply to hosting platforms. Hosts -- ranging from large commercial operations like Facebook or

---

[142] GDPR Art. 83.1.

[143] *See* Section III.E., DPAs can also carry out far-reaching audits of regulated companies, including compelling the production of information and documents. GDPR Art. 58.

DailyMotion to local news forums – support a tremendous amount of speech by ordinary Internet users. That expression will be threatened if the GDPR's new RTBF rules apply to it. As this Section will discuss, this is an open legal question. There are good arguments against requiring hosts to honor RTBF requests. But the real-world motivation of the actors involved – including both OSPs and regulators – may nonetheless push hosts toward RTBF removals.

Doctrinally, the existence of RTBF obligations should turn on whether a host counts as a Controller – defined in the GDPR as an entity that "determines the purposes and means of the processing of personal data."[144] As discussed in Section II.C, classing hosts as Cotnrollers raises real problems, seemingly subjecting them to obligations they cannot fulfill. The scant case law applying *Google Spain* to hosting platform defendants to date has not clarified matters. At least one court has held that a host – Google's Blogger service – was a Processor, not a Controller, for material uploaded by its users.[145] At least one other court has accepted that Facebook did count as a Controller.[146] And a third court (in a pre-*Google Spain* ruling), held that a host was a Controller at some times but not others.[147]

The *Google Spain* opinion does not tell us whether the RTBF applies to hosts, but it provides some important clues. The Court's analysis focuses on a form of processing

---

[144] GDPR Art. 4.7. The Article 29 Working Party's 2010 opinion identified some but not all hosts as Controllers under the similar standards of the 1995 Directive. *Article 29 Controller/Processor Opinion*, *supra* note 79. *See also* van Hoboken, *supra* note 135, at 8 (discussing complexity of assessing Controller status for social media OSPs).

[145] *See* Case 70/2015, 1st Section Audencia National, http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7309398&links=28079230012014100466&optimize=20150302&publicinterface=true (reversed on other grounds); Miquel Peguera, *Spain: The Right to Be Forgotten Does Not Apply to Blogger* (Mar. 4, 2015, 9:01 AM), http://cyberlaw.stanford.edu/blog/2015/03/spain-right-be-forgotten-does-not-apply-blogger. *See* Miquel Peguera, *Clash between different chambers of the Spanish Supreme Court on the Right to Be Forgotten* (Apr. 11, 2016) https://ispliability.wordpress.com/2016/04/11/clash_bewteen_different_chambers/.

[146] CG v. Facebook Ireland Ltd & Anor [2016] NICA 54 (Dec. 21, 2016) (accepting party stipulation). http://www.bailii.org/nie/cases/NICA/2016/54.html.

[147] *Milan Public Prosecutor's Office v Drummond*, 5017/14 12th December 2013, http://www.dirittoegiustizia.it/allegati/15/0000063913/Corte_di_Cassazione_sez_III_Penale_sentenza_n_5107_14_depositata_il_3_febbraio.html (discussed *infra* Section IV.B).

unique to web search engines: generating search results, aggregated from different sources across the web, to create a "more or less detailed profile" of an individual.[148] The Court said that this *de facto* profile was "liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page."[149]

This focus on search results shaped the *Google Spain* remedy. The Court required Google to remove data from "the list of results displayed following a search made on the basis of a person's name[,]"[150] but Google did not have to delete its own hosted copies of the data or delete the same results for other search queries. This is less than plaintiff had asked for: he wanted to completely "prevent indexing of the information relating to him personally," so that it would "not be known to internet users."[151]

The Court also emphasized that, when the law requires a search engine to erase links to a page, that does *not* mean that data on the underlying web page must also be erased.[152] This was the case for the Spanish newspaper page at issue in the case itself, in fact.[153] The Court distinguished Google from the website based on the latter's potentially stronger "legitimate interests justifying the processing[.]"[154] Preserving information on web pages – be they self-published or hosted -- protects expression and information rights in particular. Indeed, Data Protection regulators have said that Google delistings do not

---

[148] *Google Spain*, *supra* note 2, at para. 33.

[149] *Id.* at para. 80, 87.

[150] *Id.* at Rul. para. 3.

[151] *Id.* at para. 20.

[152] *Id.* at para. 82-88. The website in *Google Spain* was a news site eligible for special journalistic protections under Data protection law, but with respect to the data at issue in the case it effectively acted as an intermediary – publishing content created by the government, at the direction of the government, rather than publishing its own reporting. *See* discussion in Peguera, *supra* note 3, at 523 n. 70, 524 n. 74.

[153] *Google Spain*, *supra* note 2, at para. 82-88.

[154] *Id.* at para. 86.

significantly threaten these rights precisely *because* information is still available on the webpage.[155]

Free expression advocates may disagree and argue, as the International Federation of Library Associations and Institutions did, that "if certain search results are hidden or removed from search results, this has much the same effect as deleting the original content."[156] But deleting information at its source does still more harm, potentially eliminating it from the Internet completely. As human creative output moves to the cloud, hosts increasingly will hold the author's only copy of her own work.[157] Erasing the hosted copy could delete all traces of her expression – a drastic remedy, and one that has been rejected by the ECHR in other situations even for clearly unlawful material.[158]

Following *Google Spain*, one possible conclusion is that hosts cannot have RTBF obligations because they do not carry out the kind of "profiling" that triggered RTBF obligations for Google. The balance of rights and interests identified by the Court also plays out very differently for hosts: they typically create lesser privacy harms for data subjects,[159] and serve a more essential role for expression and information rights.[160]

---

[155] *Article 29 Google Spain Guidelines*, *supra* note 87, at 2.

[156] Gerald Leitner, *Application of Right to be Forgotten Rulings: The Library Viewpoint*, INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS (24 Oct, 2016), http://www.ifla.org/files/assets/faife/statements/161024_ifla_on_rtbf_case_in_france.pdf.

[157] 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. Fiona Macdonald, *Google's deleted an artist's blog, along with 14 years of his work,* (July 18, 2016), http://www.sciencealert.com/google-has-deleted-an-artist-s-blog-with-14-years-of-his-work.

[158] Wegrzynowski and Smolczewski v. Poland, Appl. No. 33846/07, E.Ct.H.R. (July 16, 2013), http://hudoc.echr.coe.int/eng?i=001-122365 (news articles held defamatory should not be purged from archives, other remedies such as annotation suffice). It wrote, "[t]he Court accepts that it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations." *Id.* at para. 65.

The idea that even illegal writings should be preserved for experts or posterity has an interesting history in the German library tradition of the *Giftschrank* or poison cabinet – a storage place for banned books, many of which were later restored to circulation. Sam Greenspan, *The Giftschrank* (Mar. 8, 2016), http://99percentinvisible.org/episode/the-giftschrank/

[159] *Google Spain*, *supra* note 2, at para. 80, 89.

[160] *Id*. at para. 86.

Another possible interpetation is that hosts trigger RTBF obligations when they let users search hosted content for names, generating a search result "profile" based on content stored on the host's servers. If that were correct, and if Twitter were a Controller, it would not have to delete my tweet about Matilda Humperdink -- but it might have to de-list it from results in the Twitter's search box. The Article 29 Working Party disapproved this interpretation in its *Google Spain* Guidelines.[161]

A final possibility is that hosts have some form of RTBF duties, but that they are limited compared to those of search engines because of the different balance of rights. This could mean any number of things in practice. At a minimum, they would comply with fewer RTBF requests – because, under *Google Spain*, a website can legitimately process data even when a search engine may not.[162]

In summary, no one knows whether the RTBF applies to hosts, and no one knows what hosts' erasure obligations would look like if it did. Like other open questions in the GDPR, this one is a problem precisely because it is open, leaving both regulators and OSPs relatively unconstrained in their interpretation.

As a practical matter, hosts that receive RTBF requests will have two options. One is to keep the challenged content online, and risk being summoned before a DPA. If the DPA decides that the host is a Controller, it will then be subject not only to RTBF obligations, but to the daunting array of other requirements applicable to Controllers. The host's other option is to acquiesce to the RTBF request and avoid this risk. In the absence of any transparency requirements, this host could do so inconspicuously, without acknowledging any Controller status or legal obligation, by classing the removal as voluntary.

---

[161] *Article 29 Google Spain Guidelines, supra* note 87, at 8.

[162] *Google Spain*, *supra* note 2, at para. 80; *see* discussion *infra* Section III.C.3 (discussing erasure standards and technical implementations for hosts).

Regulators, meanwhile, have institutional incentives to favor RTBF obligations for hosts. Classing hosts as controllers increases the effective authority of DPAs, and gives them means to help genuinely aggrieved people.[163] The political calculus favors deeming hosts Controllers when the opportunity arises.

As a practical matter, then, Controller status for hosts may be inevitable. Many questions (a host of questions, you might say) will then arise about how the substantive and procedural RTBF rules for hosts may differ from the ones for search engines.

C. Notice-and-Takedown Process

This section will walk through an intermediary's steps in response to a RTBF request, and explain how they systematically favor the rights of claimants asserting Data Protection rights over those of other Internet users – including those Internet users' own privacy rights, as well as information rights.

These steps are not laid out in a single section of the Regulation, but can be cobbled together from various provisions – many of them ambiguous. Some are not spelled out, but can be inferred from regulators' interpretations of similar provisions in pre-GDPR law. They are generally sensible for back-end data removals, such as requests to delete accounts, logs, or profiles, but unreasonable when applied to online expression.

Following the GDPR's apparent requirements, an OSP would follow these steps.[164] Each is discussed in detail in this Section.

1. The OSP receives a RTBF request, and perhaps communicates further with the requester to clarify what is being sought.
2. If the data subject requests it, the OSP may temporarily suspend or "restrict" the content so it is no longer publicly available -- before actually assessing the erasure request.

[163] Regardless of the host's Controller status, people with valid claims such as defamation could still get judicial relief.

[164] *See also* Ausloos & Kuczerawy, *supra* note 3, at 17-25 (discussing EU Intermediary Liability law considerations for *Google Spain* removal process, including issues of transparency and webmaster notice).

3. The OSP assesses the RTBF request to decide if it states a valid claim for erasure. For difficult questions, the OSP may be allowed to consult with the user who posted the content.
4. For valid claims, the OSP de-lists or erases the content. For invalid claims, it may bring the content out of "restriction" and reinstate it to public view.
5. The OSP informs the requester of the outcome, and communicates the removal request to other Controllers processing the same data.
6. If the data subject requests, the OSP discloses any contact details or identifying information about the user who posted the now-removed content.
7. In most cases, the OSP is not allowed to tell the accused user that her content has been de-listed or erased, and can give her no opportunity to object.
8. The OSP can publicly disclose aggregated or anonymized information about removals, but not individual instances.

For each of these steps, an OSP's safest interpretation of the GDPR tilts the playing field toward removal, and against procedural or substantive rights for the other people whose rights are affected.

1. Removal Requests

The notice-and-takedown process begins when the data subject "objects to the processing" of information about herself.[165] She can ask the OSP to "restrict" processing by taking the data offline, "erase" the data, or both. The GDPR does not specify what information the requester must provide to set the removal process in motion. This omission, if left uncorrected, will make the process slower and less predictable for both the requester and the OSP. Clear form-of-notice requirements help claimants submit actionable requests on the first try, and tell them when the ball is in the OSP's court to respond.[166] For example, if Matilda wants my tweet erased, she should have to tell Twitter basic information like the tweet's URL, and hopefully also disclose any public interest in

[165] GDPR Art. 17.1(c).

[166] The Article 29 Guidelines for Google Spain removals contain sensible form-of-request requirements, calling for RTBF requesters to "sufficiently explain the reasons why they request de-listing, identify the specific URLs and indicate whether they fulfill a role in public life, or not." *Article 29 Spain Guidelines*, *supra* note 87 at 7. Bing's RTBF removal form also asks about the claimant's role in public life. *Request to Block Bing Search Results in Europe,* BING, https://www.bing.com/webmaster/tools/eu-privacy-request.

the tweet's contents. Without formal requirements, notice-and-takedown requests commonly omit such information.[167]

Form-of-notice requirements also tell the OSP when the request is procedurally valid, and the burden has shifted to it to begin substantive review. The GDPR requires that OSPs complete this review within one month in most cases – but it is not clear if the clock starts ticking at the moment the request arrives, or once the intermediary has enough information to meaningfully evaluate the request.[168]

The GDPR does allow the OSP to ask the data subject for identification if there is a reasonable doubt as to her identity.[169] This is important and we should hope that OSPs take on the expense and nuisance of doing it, to prevent imposters from taking down information about other people. OSPs may also reject requests that are "manifestly unfounded or excessive, in particular because of their repetitive character."[170]

2. Temporarily "Restricting" Content

The next step is a striking departure from notice-and-takedown legal norms: data subjects can instruct Data Controllers to immediately "restrict" public access to information, taking it offline *before* determining whether the RTBF erasure request is valid.[171] This provision could compel OSPs to block access to blog posts, tweets, search results, and other user-generated information – even for claims that later prove to have no basis in

[167] Urban et al, *supra* note 19.

[168] GDPR Art. 12.3

[169] GDPR Art. 12.6

[170] GDPR Art. 12.5. An intermediary that rejects a request on this basis assumes the burden of proof for its conclusion.

[171] The GDPR's pre-removal restriction requirement has no analog in any major Intermediary Liability law, including the US DMCA and the EU eCommerce Directive. *See* 17 U.S.C. § 512; discussion of EU eCommerce Directive's "knowledge" standard *supra* Section II.A. These laws typically give OSPs a window of time to assess the allegation and reach a reasoned decision.

law.[172] In some cases, this temporarily removal could deprive Internet users of vitally important information – for example, about a corrupt politician on the eve of election; an embezzler meeting a new client; or a convicted abuser looking for a date. But even outside these scenarios, applying restriction requirements to online expression raises grave concerns.

a) Triggers for Restriction

The GDPR lists several situations in which data subjects can compel Controllers to "restrict" content. One is when "the accuracy of the personal data is contested by the data subject, for a period enabling the Controller to verify" its truth.[173] So, for example, Matilda could invoke this provision by claiming my tweet is false. This is a remarkable departure from the rules that would protect online expression against an identical claim of falsity under defamation and ordinary Intermediary Liability laws.[174] As applied to OSPs, this provision is also wildly impractical. OSPs have no reasonable means to "verify the accuracy of the personal data" in communications like my tweet. If restricted information can be reinstated only once an OSP has somehow unearthed the facts about a real-world dispute, it will not be reinstated.[175]

The GDPR's second basis for restriction is broader. It applies when the Controller is processing data based on "legitimate interests."[176] As discussed in Section II.C, the

---

[172] This problem intersects with the lack of form-of-notice requirements: if a requester can get information restricted without even providing information adequate to permit substantive review of her claim, potential for abuse is particularly high.

[173] GDPR Art. 18.1(a).

[174] *See* discussion *supra* Section II.A.; Testimony of Gabrielle Guillemin, *supra* note 134.

[175] The Article 29 Working Party *Google Spain* guidelines suggest that not even DPAs should try to resolve disputed facts, because, although competent to assess Data Protection issues, they are generally "not empowered and not qualified to deal with information that is likely to constitute … slander or libel," and should instead refer the issue to courts. *Article 29 Google Spain Guidelines*, *supra* note 87, at 17.

[176] GDPR Art. 18.1(d). This rule must be pieced together from several sections of the Regulation. OSPs that are regulated by the GDPR may lawfully process personal data "only if and to the extent that" one of six justifications applies. GDPR Art. 6.1. The justification for OSPs processing user-generated content that refers to another person is usually 6.1(f), which allows "processing [that] is necessary for the purposes of the legitimate interests pursued by the controller or by a third party[.]" A data subject can object to any

"legitimate interests" basis underlies almost all OSP processing of user-generated content. So this provision lets claimants demand restriction for practically any RTBF request.

Restricted content stays offline pending an OSP's later, and final, evaluation of the erasure request. Such content may,

> with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.[177]

The scope of the exception for protection of Internet users' rights is, as will be discussed in the next section, unclear.

b) Exceptions to Restriction

When can an OSP reject a restriction request and keep content online for "the protection of the rights of another natural or legal person"?[178] One possible answer is: every time. Essentially all RTBF requests affect someone's rights to seek and impart information, and arguably their rights to procedural fairness in the face of state-mandated action. OSPs restricting content based on a bare allegation would carry out a sort of privatized prior restraint, suppressing expression before deciding if the GDPR's erasure requirements even apply. On this reasoning, the restriction provision might never apply to online content, and be relevant only for requests to erase back-end data.

---

processing that is done based on this 6.1(f) "legitimate interests" justification, by invoking rights under GDPR Article 21.1. If she objects "pursuant to Article 21(1)," then she can compel Controllers to restrict the data under the provision, Article 18.1(d), discussed in the main text.

[177] GDPR Art. 18.2. *See also* GDPR Art. 4.3 (defining restriction as "the marking of stored personal data with the aim of limiting their processing in the future").

[178] Another potential basis is Article 12.5, which says that an intermediary may "refuse to act" on requests that are "manifestly unfounded or excessive."

The other possibility is that OSPs must apply the "protection of the rights of another natural or legal person" standard to restriction requests on a case-by-case basis. The meaning of the standard is unclear. Logically, it must mean something different from the standard for actual erasure – which, as discussed in the next Section, requires the OSP to assess whether "compelling legitimate grounds" justify keeping the content online.[179]

The GDPR restriction requirement shifts an important burden. Instead of an accuser having to say why expression should be prohibited – as should be required under the eCommerce Directive's "knowledge" standard for OSP removal, or in court – the GDPR gives the *OSP* the burden to identify reasons it should be permitted. The difference between these two standards in many OSPs' daily operations today may, admittedly, be slight. But for advocates concerned with improving private notice-and-takedown practices – and having a clear legal basis on which to do so -- it is important.

3. Permanently "Erasing" Content

a) Deciding If Removal is Appropriate

The intermediary now comes to the crux of the issue: determining whether to erase the content.[180] The criteria for this decision rest on the already-overburdened idea of "legitimate" interests. In various sections, the law tells OSPs to honor erasure requests unless:

- There are "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject;"[181]

---

[179] GDPR 21.1.

[180] GDPR. Art. 17.1 (Controller has "obligation to erase [the] personal data without undue delay"). According to the Article 29 Working Party, in difficult cases the intermediary may at this stage consult with the "original editor" of the information. *Article 29 Google Spain Guidelines, supra* note 87, at 3. As will be *discussed infra* Section III.C.4.c, however, this exception has limited practical value.

[181] GDPR Art. 21.1. Other grounds for declining to erase data are listed in Article 21.1 and in Article 17.3, but few are likely to apply in the RTBF context.

- There are "overriding legitimate grounds for the processing;"[182] or
- Keeping the content available is necessary "for exercising the right of freedom of expression and information."[183]

How are OSPs to know what these standards mean for RTBF requests? Search engines can look to the slowly developing body of law and guidance for their unique "de-listing" obligations under *Google Spain*.[184] Assuming the GDPR does not alter that standard, they can continue to apply the same rules.[185]

But other OSPs, including social media and other hosting platforms, have no comparable guidance.[186] They should not apply rules developed for search engines -- as discussed above, it should be *harder* to get content removed from a hosting platform, because the balance of rights and interests is different. Even if Google has to remove my tweet, for example, Twitter might lawfully continue hosting it.[187]

---

[182] GDPR Art. 17.1(c)

[183] GDPR Art. 17.3(a).

[184] *See* cases cited in Peguera *supra* note 3; Kulk & Borgesius, *supra* note 114. Regulatory guidance includes the *Article 29 Google Spain Guidelines*, *supra* note 87.

[185] There are interesting minor deviations between the GDPR and the 1995 Directive interpreted in *Google Spain*, raising the question whether aspects search engines' removal obligations under that case have changed. For example, the GDPR does not repeat the Court's "preponderant interest of the general public" standard for rejecting RTBF requests. *Compare Google Spain*, *supra* note 2, at 79 *with* GDPR 21.1 (Controller must demonstrate "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject").

[186] Guidance about "legitimate" data processing exists, but rarely involves weighing the expression rights of absent parties. *See*, *e.g.*, Article 29 Working Party, *Opinion Letter on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (Apr. 9, 2014) (WP217), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (hereinafter *Article 29 Legitimate Opinion*) (discussing obligations of OSPs processing back-end user data, but not online expression). Cases balancing rights to expression versus privacy also exist-- but those rarely involve Data Protection, or set out rules for OSPs, as opposed to ordinary publishers or speakers. *See, e.g.*, von Hannover v. Germany, App. No. 59320/00, E.Ct.H.R. (June 24, 2004), http://hudoc.echr.coe.int/eng?i=001-61853 (discussing privacy rights of public figures).

[187] This may be counterintuitive to Intermediary Liability specialists in areas such as copyright, since OSPs typically face greater liability for hosting content and lesser liability for merely linking to it. *See*, *e.g.*, Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1161-62 (9th Cir. 2007) (copyright not infringed by inline linking and framing, because content is not hosted by defendant). Those cases are different because

b) Technical Implementation of "Erasure"

Once it ascertains that a request is valid, an OSP Controller must "erase" the targeted content.[188] The word "erase" is not defined in the GDPR. But the 1995 Directive also requires "erasure," and the CJEU in *Google Spain* interpreted it to mean something relatively limited: de-listing from web search results for the data subject's name.[189] If "erase" has this nuanced, term-of-art meaning for search engines, perhaps it could be interpreted flexibly for other OSPs as well.

I have argued elsewhere that the Court based this outcome on Articles 12 and 14 of the 1995 Directive.[190] Those Articles require Controllers to honor objections only "as appropriate" and erase data only on "compelling legitimate grounds."[191] In *Google Spain*, the Court considered these obligations discharged when Google suspended some, but by no means all, of its processing activities using Mr. Costeja's data. If this analysis of the doctrinal basis for the Court's remedy is correct, then the GDPR provides the same latitude for partial, tailored implementation of "erasure." It requires Controllers to erase only where there are "no overriding legitimate grounds" to continue processing.[192]

This interpretation creates a doctrinal basis for tailoring erasure obligations of other Controllers, including OSPs. Much as Google had legitimate grounds to continue some,

---

they turn on whether a link can support liability at all – they do not address the question, posed here, about substantive standards to apply when deciding whether the content infringes claimant's rights.

[188] GDPR Art. 17.1.

[189] 1995 Directive Art. 12; *Google Spain*, *supra* note 2, at Rul. para. 3.

[190] *See* Daphne Keller, Global Right to Be Forgotten Delisting (Nov. 18 2016), http://cyberlaw.stanford.edu/blog/2016/11/global-right-be-forgotten-delisting-why-cnil-wrong.

[191] 1995 Directive Art. 12 (providing "the right to obtain from the controller . . . as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive") and Art. 14 (providing "the right… in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds… to the processing of data relating to him…. Where there is a justified objection, the processing instigated by the controller may no longer involve those data").

[192] GDPR Art. 17.1(c).

but not all, of its processing, other OSPs including hosts may have grounds to continue some of theirs. The doctrinal flexibility that led the CJEU to its *Google Spain* remedy could lead to equally tailored erasure obligations for those OSPs. For example, as discussed above, a host might "erase" information solely from results of its own on-site or in-app search function.[193] Or a social network might change settings to make a public post visible only to friends or followers, or prevent "viral" spread of information by making it harder to share a particular video within the network.[194] This leaves the technical implementation of RTBF erasure under the GDPR very much up in the air, and open to thoughtful, tailored solutions based on balancing affected parties' rights.

4. Transparency

a) Telling Controllers and the Requester

When it erases the information or otherwise takes action based on a removal request, the OSP must, reasonably, inform the requesting data subject.[195] It is also responsible for conveying information about the request to others who may be processing the data. This obligation appears twice in the GDPR. In one version, it seems to apply only to downstream "recipient[s] to whom the personal data have been disclosed."[196] In the other, it applies to a seemingly broader class of "controllers which are processing the personal data."[197]

For OSPs and their users, these requirements can lead to perverse outcomes. As an example, one important "controller which [is] processing the same data" as a search engine will be the webmaster who put that data online in the first place. But the Article

---

[193] *See* discussion *supra* Section III.B.

[194] Hosts could also justify storing copies of "erased" expression by reference to Article 17.3(e), which excuses Controllers from erasing data "to the extent that processing is necessary" for the "establishment, exercise, or defence of legal claims." It is certainly foreseeable that legal claims, against the OSP or otherwise, could arise from RTBF erasure.

[195] GDPR Art. 12.3.

[196] GDPR Art. 19. Controllers need not do so if it "proves impossible or involves disproportionate effort." *Id.*

[197] GDPR Art. 17.2.

29 Working Party has already said it thinks that Bing and Google should *not* contact webmasters in most cases.[198] Similarly, Facebook may know which users liked or shared a post, or even simply viewed it. The GDPR seems to oblige Facebook to notify these people, as "recipient[s] to whom the personal data have been disclosed" – not only about erasures, but even about failed requests that led only to temporary "restriction" of online content.[199]

Few data subjects filing RTBF requests will want this additional social media attention. If these provisions apply to OSPs, they effectively take away the data subject's freedom, emphasized by the Article 29 Working Party, to "choose how to exercise" their rights by "selecting one or several" of possible recipients for RTBF requests.[200]

These provisions are clearly better suited to traditional data Controllers -- a hospital that shares patient information with an outside physician, for example. And they seem well targeted to online actors, including OSPs, if they share back-end data about their users for purposes such as advertising. Presumably the GDPR's drafters had these kinds of data sharing in mind. But if OSPs are deemed Controllers of user-generated content, provisions like this will cover them, too – with perverse and unintended results.

b) Giving the Requester Personal Information About the Speaker

Another extremely odd GDPR provision is its apparent requirement that OSPs disclose personal information about users whose posts are targeted by RTBF requests. Such disclosure is seriously out of line with the GDPR's general pro-privacy goals, and it is hard to imagine that drafters intended them to apply in the RTBF context.

---

[198] *See* discussion *infra* section III.C.4.c.

[199] GDPR Art. 19 ("shall communicate any rectification or erasure of personal data or restriction of processing").

[200] *Article 29 Google Spain Guidelines, supra* note 87, at 7.

The requirement appears in lists of a Controller's obligations when it receives data about an individual from someone other than that individual herself. They include telling the data subject "from which source the personal data originate"[201] and "any available information as to their source[.]"[202] Applied to OSPs, for which the "source" of the data is an Internet user posting her expression online, these requirements make no sense.

If Twitter were deemed a Controller for my tweet about Matilda Humperdink, for example, the GDPR would entitle her to "any available information" about the tweet's source – which is to say, whatever Twitter knows about me. Twitter is supposed to provide this information even if it finds no legal ground to erase my tweet.[203]

Applied to OSPs, these rules seriously alter the landscape for anonymous expression, and strip online speakers of their own Data Protection rights. These sections of the GDPR, like so many others, seem crafted to apply to back-end data – not online expression.

---

[201] GDPR 14.2(f). Exceptions to this obligation are listed at 14.5, but none would appear applicable. The most promising, 14.5(c), excuses the Controller from informing the data subject of the poster's identity where "obtaining or disclosure is expressly laid down by Union or Member State law." It is tempting to read this to mean that an intermediary need not disclose a poster's identity when the law protects the *poster*'s privacy or right to speak anonymously. Unfortunately, it doesn't appear to mean that.
The 1995 Directive has similar language, requiring Controllers to tell the data subject about any disclosure of her information unless "disclosure is expressly laid down by law." 1995 Directive Art. 11. There, "expressly laid down by law" means *required* by law. As the EU Agency for Fundamental Rights explains, the idea is that Controllers don't need to tell a data subject when the law requires them to disclose her information, because she is presumed to know the law. *See* EU Agency for Fundamental Rights, *Handbook on European Data Protection Law* 97 (2014), http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf. The GDPR exception seemingly means the same thing: a Controller need not tell the data subject about things that, based on the law, she should already know. It is not an exception to the duty to tell her things she doesn't know – in particular, the identity of the person who posted information about her.

[202] GDPR 15.1(g) This section also has language that initially appears to exempt Controllers from disclosing information – in this case, based on "the rights and freedoms of others." GDPR Art. 15.4. This unfortunately only exempts Controllers from sharing a copy of the processed data, not from disclosing the data's source.

[203] Arguably, Matilda could also find out who read the tweet. Article 14.1(e) entitles her to find out "the recipients or categories of recipients of the personal data, where applicable[.]" Similarly, Article 19 says that for "each recipient to whom the personal data have been disclosed," the Controller "shall inform the data subject about those recipients if the data subject requests it." It is to be hoped that this relatively loose language gives OSPs leeway to tell the data subject "about those recipients" in general terms, without disclosing their individual personal information.

c) (Not) Telling the User Whose Expression Was Erased.

In the aftermath of the *Google Spain* ruling, the Article 29 Working Group considered whether Google should be permitted to tell webmasters when their pages were de-listed. The Group opined that "[t]here is no legal basis for such routine communication under EU Data Protection law."[204] But they said that consultation would be acceptable in unusual cases when necessary to resolve difficult requests.[205]

The question whether routine notice to webmasters violates the law under the 1995 Directive remains in dispute. The GDPR does nothing to clarify the issue. But because it does not appear to change any relevant law, presumably the interpretation of the Article 29 Working Group (or the new Board) will remain the same. If hosts are deemed to be Controllers, the same reasoning could preclude notice to their users when online expression is deleted.

Prohibiting notice to the affected online speaker makes some sense from a pure Data Protection perspective. After all, the requester is exercising a legal right to make the OSP stop processing her information. A company that then talks to a poster, publisher or webmaster about the request is just doing more unauthorized processing. More pragmatically, a person whose privacy is violated by online content may not want the perpetrator to know of her efforts to remove it.

As a matter of procedural fairness or protection of free expression, though, taking content down based solely on an accusation, with no notice to the accused or opportunity for defense, raises obvious problems. It places the fate of online expression in the hands of accusers and technology companies – neither of whom has sufficient incentive to stand up for the speaker's rights. That's why notice to the accused, and an opportunity to reply, is so central to the Manila Principles and many civil society standards for Intermediary

---

[204] *Article 29 Google Spain Guidelines, supra* note 87 at 3, para. 9.

[205] *Id*. at 3.

Liability rules.[206] The CJEU has even required EU Member States to give Internet users judicial recourse in cases of OSP over-removal in some situations, saying that this correction mechanism is necessary to protect information access rights.[207]

Involving the content creator also opens up possibilities for better-tailored solutions to online privacy violations. OSPs typically face a binary choice – take content down or leave it up. [208] But a content creator can do much better: she can reword a phrase, update or annotate a news story, or take down one sentence of a blog post while leaving lawful text intact[209] Webmasters can also use technical tools to control whether search engines index their pages.[210]

In the reasoning of the *Google Spain* Guidelines, OSPs should contact publishers only in special cases, where their input is needed to resolve a removal request. In practice, such a limited exception only protects Internet users' rights if OSPs themselves accurately identify flawed notices – and initiate individual communication about each one. That approach defeats a key purpose of notifying the affected publisher: correcting for errors

---

[206] *See* discussion *supra* Section II.A.

[207] Telekabel, 62012CJ0314, at para. 57 (when courts order ISPs to block websites without specifying technical means of doing so, potentially leading to over-blocking of lawful information, "national procedural rules must provide a possibility for internet users to assert their rights before the court once the implementing measures taken by the internet service provider are known.")

[208] There are other logical possibilities, but most – like taking a scene out of a hosted video – would endanger the intermediary's protections under the EU eCommerce Directive or other Intermediary Liability laws. C-236/08, Google France v. Louis Vuitton 2010 E.C.R. I-02417.

[209] These practical remedies are closely analogous to those sometimes offered by press archives, such as allowing annotation, rectification, or reply to inaccurate articles.

[210] Some authorities have encouraged or required webmasters themselves to use technical tools to prevent indexation based on Data Protection obligations. *See*, *e.g.*, *Article 29 Legitimate Opinion, supra* note 186, at 58-59 (news archives may balance data protection and free expression rights by using technical tools to block indexation; *c.f.* Ausloos and Kuczerawy, *supra* note 3, at 10 (Belgian court rules publishers must sometimes prevent indexation); *Il Garante Per La Protezione Dei Dati Personali*, Italian Data Protection Authority, Decision, Doc. 1583162 (Dec. 11, 2008), http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1583162 (*discussed in* Aurelia Tamò and Damian George, *Oblivion, Erasure and Forgetting in the Digital Age*, 5 (2014) JIPITEC 71at f.n. 121-123) (Italian DPA requires news archive to block indexation). The Constitutional Court of Colombia reached a similar outcome in a post-*Google Spain* case assessing RTBF under Colombia's data protection law. Constitutional Court, On behalf of a minor vs. "El nuevo día" newspaper & Instituto Colombiano de Bienestar Familiar, Judgment T-453/13, (July 15, 2013) (Colom.) http://www.corteconstitucional.gov.co/relatoria/2013/T-453-13.htm.

made by the OSP itself. For example, if Twitter does not know that Matilda Humperdink's party was a commercial restaurant opening, it may not recognize any public interest in my tweet about her food making people sick. By contrast, if notice to accused speakers is a standard practice, and not an exceptional step instituted by the OSP, the opportunity for error-correction is put in the hands of the person best motivated and equipped to use it.

d) Telling the Public What Information Has Been Erased

The GDPR is silent on the question of transparency to the public about RTBF erasures, seeming to preserve the status quo from the 1995 Directive. That almost certainly means that OSPs can only be transparent in ways that do not identify the person who sought removal. This standard permits some established public transparency practices for notice-and-takedown, but precludes important other ones.

Transparency reports consisting of aggregated figures – number of requests received, number granted, how many came from which country, and the like – should be fine under the GDPR. So should transparency about the rules an OSP applies in assessing requests – with the exception of rules so specific to an unusual case that they would effectively identify the requesting party.

But transparency about what information has been affected by removal requests is very difficult under the GDPR. Even disclosing a page URL or file name could effectively identify the person who objected to it. This is a problem for OSPs who might otherwise post an explanatory notice to users when content they seek has been removed – like the copyright removal notices on YouTube. It also harms OSPs' ability to share copies of removal requests with public repositories like the Lumen database, operated by Harvard Law School's Berkman Center. The Lumen database archives redacted copies of legal removal requests.[211] In addition to enabling significant scholarship,[212] the database lets

[211] *See* Lumen Database, *supra* note 22.

any interested party identify when content has been removed improperly. In conjunction with OSPs' notices to users, this effectively crowd-sources the job of error correction. These important checks on over-removal will probably not be available for RTBF requests under the GDPR. It may be possible, though, for regulators to approve more limited disclosure – perhaps to academic researchers – as permissible processing of personal data from RTBF requests. The absence of more robust public transparency makes other procedural checks on over-removal all the more important.

D. Free Expression and Information Protections

1. Express General Data Protection Regulation Provisions

The GDPR lists "the right of freedom of expression and information" as a basis for OSPs to decline RTBF requests.[213] However, as van Hoboken wrote of an earlier GDPR draft, "its lack of clarity about the scope and substance of exceptions and derogations to be made in view of freedom of expression raises very serious questions."[214] While the GDPR carefully details the data protection side of this balance, it leaves individual EU member states to "reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information[.]"[215]

This is the same allocation of responsibility to Member States that exists under the current 1995 Directive, and empirical research reveals significant problems with it. Cambridge's David Erdos has exhaustively reviewed and analyzed national free expression carve-outs from data protection law, and found significant and troubling variation from one country to another.[216] Some countries have not even passed the free

---

[212] *See* Lumen Database, *supra* note 22; Brief of Amici Curiae, *supra* note 37.

[213] GDPR Art. 17.3, *see also* Recitals 4, 65.

[214] Van Hoboken, *supra* note 135, at 29.

[215] GDPR Art. 85.

[216] Erdos concludes that "many Member State laws have clearly failed to provide for an effective balance between data protection and freedom of expression in the media sphere." David Erdos, *Fundamentally Off Balance: European Union Data Protection Law and Media Expression* 3 (July 25, 2014), https://ssrn.com/abstract=2471531.

expression legislation mandated decades ago under the 1995 Directive.[217] Others have enacted laws that fall far short of the goal of balancing Expression and privacy rights. Given this history, it seems unrealistic to expect better outcomes under the GDPR.

Another problem is that while Member States are specifically required to create exemptions for "journalistic … academic artistic or literary expression," legal protections are less clear for expression that does not fall in one of these four categories.[218] That's a problem for OSPs struggling to interpret the law, because valuable online expression often falls outside of those four enumerated categories. A tweet about a dishonest car mechanic, a Yelp review of a botched medical procedure, or a post criticizing an individual Etsy or Amazon vendor may not be covered. Neither might a personal blog post recounting domestic abuse. This kind of material appears to be a far cry from the privileged – and often professionalized and even licensed – categories of expression listed in Article 85.2.[219] But it is precisely this democratic cacophony that makes the Internet so different from prior speech platforms. Without clear free expression protections to guide OSPs, this speech is at risk.

Also troubling is the GDPR's lack of clarity about *whose* free expression rights an OSP should consider. The most obvious person should be the publisher or Internet user who posted the content. But doctrinally and before courts, serious legal uncertainty can arise regarding an intermediary's ability to act on the basis of that user's rights -- as opposed to

---

[217] *Id.* at 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.") (internal citations omitted)

[218] GDPR Art. 85. For the four enumerated categories of expression, the GDPR requires that Member States "shall provide for exemptions or derogations" and notify the Commission of "the provisions of its law which it has adopted" – suggesting countries must enact written laws on point. *Id.* at Art. 85.2-3. For other kinds of Free Expression, Member States need only "by law reconcile" the rights, which might just mean requiring judges to consider them. *Id*. at Art. 85.1. *See also* David Erdos, *From the Scylla of Restriction to the Charybdis of License? Exploring the Present and Future Scope of the 'Special Purposes' Freedom of Expression Shield in European Data Protection*, Common Market Law Review 52: 119–154, 2015 (exploring tensions between the special purpose Free Expression provisions in the draft GDPR and its Data Protection provisions).

[219] *See generally* Van Hoboken, *supra* note 135, at 23 (discussing role of "doctrines that were traditionally reserved for the institutionalized press" in context of blogs and other non-professionalized expression); Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, 2008 E.C.R. I- 09831, ¶ 56-62 (applying journalistic exemptions broadly to "disclosure to the public of information, opinions or ideas.")

the company's own, relatively paltry, free expression rights. As a conspicuous example, the CJEU's *Google Spain* ruling itself did not identify the publisher's expression rights as a balancing factor that Google should consider in removing search results. Even the ECHR, in one Intermediary Liability case, appeared to base its analysis on the rights of the OSP – though in a later case it shifted focus to the platform's users.[220] Internet users' rights should be a central concern of notice-and-takedown systems, and OSPs, regulators, and courts should expressly take them into consideration.

Data protection law's lack of detailed provisions for free expression made sense in an era when regulated data consisted of records held by banks, employers, medical offices, and the like. With Data Protection emerging as a major law governing users' speech on Internet platforms, however, uncertainty about these protections will chill legitimate online expression. The law's own inadequacies will ramify as it is interpreted by risk-averse private companies under the GDPR's notice-and-takedown framework. Unfortunately, as will be discussed in the next section, public adjudication and regulatory review may do little to correct for this imbalance.

2. Enforcement Processes

The processes for courts and regulators to resolve disputes involving privacy and free expression under the GDPR are significantly imbalanced.[221] A person asserting a privacy or data protection right has state support and a clear avenue to enforce her rights. A person asserting a countervailing free expression right does not. In this respect, public adjudication by DPAs and courts has many of the same systemic imbalances as the GDPR's private notice-and-takedown process

---

[220] *Compare* Delfi, (2015) E.Ct.H.R. 140, 162 with MTE, (2016) E.Ct.H.R. 36-39, 61, 82, 86, 88; *see also* Daphne Keller, *Litigating Platform Liability in Europe: New Human Rights Case Law in the Real World* (April 13 2016, 5:00 AM), http://cyberlaw.stanford.edu/about/people/daphne-keller.

[221] The ECHR has spoken to the importance of judicial review to avoid over-removal of lawful online content. Ahmet Yildirim, App. No. 3111/10, E.Ct.H.R. para. 68 (site blocking violates Convention rights where "the judicial- review procedures concerning the blocking of Internet sites are insufficient to meet the criteria for avoiding abuse, as domestic law does not provide for any safeguards to ensure that a blocking order in respect of a specific site is not used as a means of blocking access in general."); *see also* Telekabel, 62012CJ0314.

The basic sequence of events is as follows. When an intermediary does not comply with a RTBF removal request, the requester can take her grievance to the regional or national DPA.[222] For example, if Twitter declines to remove my tweet and Matilda lives in Sweden, she could complain to the DPA there. The DPA adjudicates the matter as a two-party dispute between the data subject (Matilda) and the intermediary (Twitter), typically under strict rules of confidentiality.[223] The person whose free expression rights are at stake – in our example, me -- is typically absent from the process.[224] The unknown Internet users and potential restaurant diners who might benefit from reading the tweet are of course also absent. Defending their rights before the DPA falls to the OSP, which likely doesn't know if the review is telling the truth, and has little incentive to litigate on the user's behalf.

DPAs' mandate nominally extends beyond data protection: they are "to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union."[225] In practice, DPAs have shown real sensitivity to free expression concerns, including in the thoughtful RTBF public interest criteria released by the Article 29 Working Party.[226] But DPAs remain, in most cases, bodies of privacy professionals (not necessarily lawyers) whose job is to regulate the processing of personal data. Absent a far stronger legal mandate for them to balance privacy with free expression, and without including free expression experts as important actors within the agencies, it is not reasonable to expect DPAs to be equally attuned to both sets of rights. This natural focus on the privacy side of the equation can

---

[222] GDPR Art. 77. GDPR Art. 79 allows her to also go directly to a court.

[223] GDPR Art. 54.2.

[224] There is an interesting question about what happens if an intermediary has accepted the Article 29 Working Party's authorization to contact the affected speaker in particularly difficult removal cases. *Article 29 Google Spain Guidelines*, *supra* note 87, at 10. Can that person then be included in any subsequent procedure before a DPA?

[225] GDPR Art.51.1. Note that this mandate is broader than the one DPAs held under the 1995 Directive. *See* 1995 Directive Art. 28.

[226] *Article 29 Google Spain Guidelines, supra* note 87, at 12-20.

only be amplified when the person asserting a privacy harm stands before them, while the person who might suffer a free expression harm is nowhere to be seen.

Under pre-GDPR data protection law, regulatory review of a rejected RTBF claim would typically end with the DPA. At that point either the data subject or the intermediary could move the dispute to national court.[227] The GDPR changes this by adding another potential level of regulatory review, under the new EU Data Protection Board.[228] The Board will review cases and issue opinions to harmonize differences in cases of disputes between national DPAs – differences which, in the free expression context, may easily arise from divergent Member State law. For example, the Swedish DPA might agree with Twitter that the public has an interest in knowing about Matilda's dangerous food. But if a factually similar case arose in Estonia, that DPA might think the Data Protection interests are stronger.[229] When the Board reviews such a dispute, just as when a DPA does, there is no apparent notice to or role for the Internet user whose online speech is being assessed.

Oddly, one GDPR Recital suggests that Member State courts may not review Board decisions, including those balancing free expression and privacy rights.

> [W]here a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice[.][230]

So if the Swedish and Estonian DPAs disagreed about Matilda's complaint or about the principles governing complaints of that type, the issue could potentially be resolved by the Board. One or both national DPAs would resolve disputes or issue orders on the basis of its decision. A Swedish court reviewing those orders would seemingly not be

---

[227] 1995 Directive Art. 28.3.

[228] GDPR Art. 65.

[229] The GDPR's provisions to allocate responsibility and coordinate among national DPAs are unlikely to resolve this issue. *See* discussion *infra* Section III.E.

[230] GDPR R. 143.

permitted to nullify the Board's decision, even if it conflicted with Swedish free expression law as interpreted by the court. Following this strange avenue, a dispute about the balance between Data Protection and information rights could in theory make it all the way to Europe's highest court without the core information rights issue ever being resolved by a judge in a Member State. This avenue would make sense if the GDPR were a purely harmonized, EU-wide legal framework. But it isn't: the GDPR expressly leaves free expression protections to Member States, preserving national differences in this area of law. That makes the potential exclusion of Member State courts from the Data Protection / free expression balancing exercise very troubling.[231]

A dispute that made its way to the CJEU by this means would also apparently exclude the affected original publisher. As in the *Google Spain* case, the Court would hear argument from the intermediary only.[232]

By contrast to this multi-stage process for a claimant raising a privacy right, the legal path for a claimant raising a free expression right under RTBF is short and disappointing. Regulatory review is typically not an option. No publicly funded, legally powerful "Information Rights Agency" stands as an institutional counterweight to DPAs. In most cases, an Internet user or publisher's 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 countries, there is no clear cause of action against an individual whose claim led an intermediary to remove content, or against the intermediary for taking that accusation at face value.[233] Publishers, speakers, and Internet users deprived of access to information under the GDPR may have no remedy.[234]

---

[231] One alternate interpretation of the provision is that national courts can require national DPAs not to comply with Board decisions, but cannot overrule the Board itself. Another is that the national court could consider the case, but only after a CJEU referral. Either seems odd.

[232]La Vanguardia was initially a party to *Google Spain*, but ceased to be when the Spanish DPA determined that its processing was lawful. Peguera, *supra* note 3 at 524.

[233] The CJEU has said that Internet users have standing to contest over-removal in at least some cases when it results from a court order. Telekabel, 62012CJ0314. For cases not involving court orders, the idea of legal remedies for "wrongful removal" is increasingly discussed in the human rights literature. *See, e.g.*, Rep. of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and

E. Jurisdiction

A final threat to free expression rights comes from the GDPR's extraterritoriality provisions.[235] These are deliberately expansive, applying EU Data Protection law to many foreign actors in order to more effectively protect European privacy rights. To the extent GDPR leads to unintended harms to the information and privacy rights of people who post content online, that harm will be exported through application of EU law to information shared in other countries.

1. Prescriptive Jurisdiction: Who Must Comply?

The GDPR expands the reach of EU Data Protection Law in several ways.[236] Most importantly, it covers entities outside the EU if they process personal data of EU users "in relation to" the "monitoring of their behavior."[237]

---

expression, at 52, 67-71, U.N. Doc. A/HRC/32/38, (May 11, 2016); Council of Europe *supra* note 13. But the doctrinal basis for such a claim in national laws remains unclear. One French case raising this claim received publicity in 2016 but did not reach a reported ruling on the merits. *See Paris Court Rules Against Facebook in French Nudity Case,* BBC (Feb. 12, 2016) http://www.bbc.com/news/world-europe-35559036. In the US, multiple "wrongful removal" cases have been rejected by courts. *See, e.g.*, Lewis v. YouTube, H041127, 2015 WL 9480614 (Cal. App. Ct. Dec. 28, 2015); Darnaa, LLC v. Google, Inc., No. 15-cv-03221-RMW, 2015 WL 7753406 (N.D. Cal. Dec. 2, 2015); Song Fi v. Google, Inc 108 F.Supp.3d 876 (N.D. Cal. 2015).

[234] The GDPR does interestingly provide that "each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them." GDPR Art. 78.1. Arguably, this should open the door for an affected speaker to get into court once a DPA orders an OSP to delete her speech, even if she was not a party before the DPA.

[235] Territorial application of EU Data Protection law is complex and largely beyond the scope of this Article. It is well examined in Michel Jose Reymond, *Hammering Square Pegs into Round Holes: The Geographical Scope of Application of the EU Right to Be Delisted*, BERKMAN KLEIN CTR. R. PUB. NO. 2016-12 (2016).

[236] GDPR Art. 3.2. Because extraterritorial application of the 1995 Directive is disputed, some practitioners may argue that EU Data Protection law always applied this broadly.

[237] GDPR Art. 3.2(a). Another new provision applies the GDPR to entities engaged in "the offering of goods or services… [to] data subjects in the Union." GDPR Art. 3.2(b). This basis for jurisdiction is relatively cabined by a Recital explaining that mere accessibility of a site to EU users does not establish jurisdiction, and that factors like the language of the site or the currency used for transactions should be considered. GDPR R. 21. *See also* Michel Reymond, *Jurisdiction in case of personality torts committed over the internet: a proposal for a targeting test*, 14 Y.B.PRIV. INT'L L. (2013) 205-246 (discussing "targeting" jurisdiction analysis in the EU).

"Monitoring" is not defined in the GDPR, but a recital explains that it includes tracking a data subject for purposes of "profiling," including "predicting her or his personal preferences."[238] "Profiling" *is* defined, and very broadly. It means

> any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[239]

This definition would appear to cover standard online customization, like the articles recommendations for individual users in the New York Times online, as well as individually targeted advertising. For the untold number of entities with features like these, serving EU users will likely mean falling under the GDPR.[240] The extraterritorial effect is still greater if "monitoring" covers standard web analytics programs that track IP addresses of users.

Where does all this really leave non-EU companies that do business online? For large companies that already offer services to European markets and have invested in compliance with current Data Protection law, the transition will take work but should not pose insurmountable difficulties. For smaller companies that have never operated in the EU, the picture is very different. Realistically, the GDPR may never actually be enforced against them. On the other hand, complaints from disgruntled users, whether valid or invalid, could at any time bring regulatory attention and potentially high fines even to obscure or distant entities. So both uncertainty and actual or perceived financial exposure are high.

---

[238] GDPR R. 24.

[239] GDPR Art. 4.4.

[240] There is room for argument that jurisdiction does not attach unless an OSP intended to monitor EU users. *See* Lindqvist, 2003 E.C.R. (applying an intent standard for data transfer provisions under the 1995 Directive). Once an EU user communicates a RTBF request to an OSP, though, it arguably knows of and intends to monitor that user.

2. Territorial Scope of Compliance: Must OSPs Erase Content Globally?

Once an entity is subject to RTBF obligations under the GDPR, must it comply globally by erasing content for users all over the world – even in countries where the material is legal? The GDPR does not directly address this question. The pre-GDPR version of this issue, however, gained considerable public attention in 2016, when the French DPA ordered Google to de-list search results globally based on French RTBF law.[241] Google maintained that it only needed to comply with this law on its services targeted to Europe, since citizens of other countries have rights to access the de-listed information under their own national law. Resolution of this case, which arises under the 1995 Directive, will likely shape outcomes under the GDPR – including outcomes for hosts and other OSPs.

This is not solely a matter of conflict between EU and non-EU law. The same questions arise when law varies between EU Member States, as it inevitably will. The GDPR, like the 1995 Directive, expressly contemplates that laws balancing Data Protection with free expression will not be harmonized, but will be unique to each Member State.[242] Current divergence between national laws will persist under the GDPR.[243] It is entirely foreseeable that, as described in the example of my tweet, one nation's laws might require an OSP to remove a link or content, while another's does not. Which country's law should prevail? The GDPR says it should be "the law of the Member State to which the controller is subject," but for non-EU companies with operations throughout the EU, this is unlikely to resolve the problem.[244]

---

[241] Mark Scott, *Google Appeals French Privacy Ruling*, New York Times (May 19 2016), http://www.nytimes.com/2016/05/20/technology/google-appeals-french-privacy-ruling.html?_r=0; *see also* D. Keller and B. Brown, *Europe's Web Privacy Rules: Bad for Google, Bad for Everyone*, NY TIMES (April 26, 2016), http://www.nytimes.com/2016/04/25/opinion/europes-web-privacy-rules-bad-for-google-bad-for-everyone.html?_r=1.

[242] GDPR Art. 85. *See* discussion *supra* Section III.D. The GDPR's ambitious new procedures to reconcile differences of opinion between DPAs and harmonize the law can't solve this problem without effectively nullifying Article 85's reservation of power to Member States to set their own Free Expression laws.

[243] Erdos, *supra* note 216, at 11 (identifying wide variation in national law balancing Data Protection and Free Expression rights).

[244] GDPR R. 153.

As with so many unresolved questions under the GDPR, this one creates systematic pressure in favor of more content removal. If RTBF removals must be global and Estonian and Swedish laws conflict, an OSP could face fines in Estonia for failing to remove content in Sweden. By contrast, Swedish regulators are unlikely to notice or react if the OSP removes the content in order to avoid legal trouble in Estonia. If this dynamic persists, national law favoring deletion can be expected to consistently trump other countries' laws favoring user expression.

IV. Relation to Notice-and-Takedown Rules of the eCommerce Directive

Internet users and OSPs could be spared the GDPR's problematic takedown rules through a seemingly simple legal move: applying the EU's existing Intermediary Liability laws under the eCommerce Directive. I will refer to the procedural rules derived from the Directive itself, Member State implementing legislation, and interpreting case law as "eCommerce Rules." These rules provide far more balanced protections than the "GDPR Rules" discussed above.[245] Importantly, a key GDPR provision suggests that the GDPR's drafters actually intended to invoke and apply the eCommerce Directive. If this is the case, and eCommerce Rules *do* cover RTBF removals, then many of the problems I identified with the GDPR Rules are solved. The GDPR Rules would remain effective and meaningful, but apply only to erasure of stored back-end data such as logs or profiles.

Unfortunately, as will be discussed in this Section, doctrinal conflicts could prevent this outcome. The law on point is messy, with arguments on both sides. As with so many of the GDPR's ambiguities, this one creates bad incentives for OSPs to play it safe by accepting the interpretations that most favor removal, and that least protect other Internet users' rights.

---

[245] *See* discussion *supra* Section III.C. If eCommerce Rules do apply the GDPR, arguably only the Directive itself – and fundamental rights-based limitations – would be binding. Member state implementation and interpretation would nonetheless be relevant and useful.

A. Procedural Protections for Information Rights under the eCommerce Directive

There are a number of good reasons to apply eCommerce Rules to RTBF notice-and-takedown. One reason is for consistency and fairness among people seeking content removal. The GDPR Rules would give RTBF claimants a procedural shortcut compared to those alleging defamation, hate speech, non-Data Protection privacy torts, and other harms – all of whom must clear the procedural hurdles of the eCommerce Directive. Nothing about RTBF claims justifies this leg up over other long-established claims, including conventional civil privacy claims. The procedural advantage, combined with the ease of prevailing on RTBF requests as a substantive matter, encourages gamesmanship in removal claims and litigation.[246] Indeed, in the wake of the *Google Spain* case, many individuals who had previously alleged defamation or other harms re-filed removal requests and complaints under new RTBF theories.[247]

More fundamentally, the eCommerce Rules do a better job of balancing the rights of all parties affected by notice-and-takedown -- including Internet users whose free expression and information rights are affected. They do so through two key standards. First, the eCommerce "knowledge" standard for OSPs to remove unlawful user expression stands in striking contrast to the GDPR's "restriction" rule, which encourages OSPs to remove first, and ask questions later.[248] Second, the eCommerce rule against making OSPs monitor users' communications protects both information and privacy rights of Internet

---

[246] *See*, e.g., Ashley Hurst, *Data Privacy And Intermediary Liability: Striking A Balance Between Privacy, Reputation, Innovation And Freedom Of Expression*, https://inforrm.wordpress.com/2015/05/14/data-privacy-and-intermediary-liability-striking-a-balance-between-privacy-reputation-innovation-and-freedom-of-expression-part-1-ashley-hurst/ (noting that using data protection claims in lieu of privacy or defamation gives plaintiffs "a potential short cut" and avoids "lengthy debate about such terms as "reasonable expectation of privacy"); Sébastien Proust, The Proposed European Regulation On The Right To Be Forgotten, Or An End To National Laws On The Freedom Of Press, 24 ENT.L.R. 207 (2013) (arguing RTBF displaces careful balance from existing laws).

[247] Author's personal knowledge.

[248] *Compare* discussion *supra* Section II.A (eCommerce "knowledge" standard) with *supra* Section III.C.2 (GDPR "restriction" standard). *See also* Ausloos & Kuczerawy, *supra* note 3, at 21-23 (discussing "manifestly illegal" standard from eCommerce discussions).

users.[249] The Directive also encourages Member States to enact additional procedural protections, as some have done.[250] By contrast, diverging national notice-and-takedown rules would arguably conflict with the GDPR's harmonization goal.[251]

Of course, the eCommerce Directive has problems of its own. Its provisions are inconsistently applied across the EU, it has too often been interpreted in ways that erode its free expression protections, and is under attack politically.[252] But it remains the EU's core Intermediary Liability law, and as a result there are real, sustained efforts underway to protect free expression online and preserve reasonable rules based on its provisions.[253] Legal gains made through this advocacy and scholarship will not benefit Internet users targeted by bad-faith or groundless RTBF requests if the eCommerce Directive does not apply to them.

In principle, it would be possible to construct a sui generis, rights-respecting notice-and-takedown framework based strictly on fundamental rights, without relying on provisions of the eCommerce Directive. If lawmakers conclude that the Directive does not apply to RTBF notice-and-takedown, this is what they will have to do. A rare few cases provide guidance for such an undertaking.[254] ECHR precedent, for example, has limited OSP

---

[249] SABAM, 2011 E.C.R.; Netlog, (2012) 2 C.M.L.R.

[250] Mylle and Mylly, *supra* note 47.

[251] Member States could arguably still enact procedural rules as part of their free expression protections. GDPR Art. 85.

[252] *See generally* Monica Horton, *Content 'Responsibility: The Looming Cloud of Uncertainty for Internet Intermediaries,* CTR. FOR DEMOCRACY & TECH. (Sept. 6, 2016), https://cdt.org/insight/content-responsibility-the-looming-cloud-of-uncertainty-for-internet-intermediaries/.

[253] *See*, *e.g.*, Sophie Stalla-Bourdillon et al, *Open Letter to the European Commission - On the Importance of Preserving the Consistency and Integrity of the EU Acquis Relating to Content Monitoring within the Information Society* (September 30, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2850483; EDRi, *Deconstructing Article 13 of the Copyright proposal of the European Commission*, https://edri.org/files/copyright/copyright_proposal_article13.pdf; Christina Angelopoulos, *EU Copyright Reform: Outside the Safe Harbours, Intermediary Liability Capsizes into Incoherence* (October 6, 2016), http://kluwercopyrightblog.com/2016/10/06/eu-copyright-reform-outside-safe-harbours-intermediary-liability-capsizes-incoherence/; Article 19, *Internet Intermediaries: Dilemma of Liability* (2013), https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf.

[254] MTE, (2016) ECtHR; Delfi, (2015) E.Ct.H.R. Angelopolous et al, *supra* note 13, at 28, argue that CJEU case law also supports the proposition that, "even absent Article 15, such a burdensome [obligation] would

monitoring obligations based purely on human rights under the Convention.[255] But far more common are cases that merge the two, usually by interpreting national eCommerce Rules in light of fundamental rights.[256] If the eCommerce Directive does not apply to RTBF removals, this case law will have only limited value.

B. Applicability of the eCommerce Directive to RTBF Removals

Until quite recently, collisions between the eCommerce Directive and Data Protection law were rare. As a result, few cases have attempted to reconcile the two. This Section reviews legal issues – some conceptual, and some arising from language in governing legal instruments -- that make such reconciliation complex. These questions will be particularly important if the problems with the GDPR's notice-and-takedown process are resolved through litigation, rather than through regulatory or Member State lawmaker action.

1. Conceptual Tensions between Intermediary Liability and Data Protection

There is a fundamental question about whether eCommerce Rules should, as a matter of principle, apply to RTBF. The answer depends in part on how we understand the purpose and function of Intermediary Liability.

From one perspective, RTBF looks like a textbook Intermediary Liability law. It tells OSPs when they need to remove content created by users. The legal obligation is content-

---

also be illegal under the EU's fundamental rights framework." (Discussing Netlog, (2012) 2 C.M.L.R.) There is also considerable "soft law" material from human rights institutions. *See, e.g.*, United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, Organization of American States (OAS) Special Rapporteur on Freedom of Expression and African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and the Internet* (June 1, 2011), http://www.oas.org/en/iachr/expression/showarticle.asp?artID=849&lID=1; Frank La Rue, para. 42 (),

[255] MTE, (2016) ECtHR.

[256] *See, e.g.*, SABAM, 2011 E.C.R. (interpreting EU eCommerce Directive Article 15 in light of fundamental rights), L'Oreal, 609CJ0324, Telekabel, 62012CJ0314.

based – it depends on what the user is saying. And the consequences for the affected user are the same as in any notice-and-takedown system: her ability to participate and share information over the Internet is curtailed or eliminated.

From another perspective, Intermediary Liability is irrelevant. As framed by Data Protection law, RTBF requests are not about holding OSPs liable for user-generated content.[257] The duty to erase arises from the Controller's own independent legal obligations – not from those of its users.[258] Data Protection law may oblige an OSP to suspend its *own* processing activities, even if those who posted the content acted lawfully, as happened with the news site in *Google Spain*.[259]

It is also debatable whether RTBF obligations should be considered a form of "liability" at all. The GDPR refers separately to Controllers' "responsibilities" and "liabilities," and seems to class RTBF obligations as the former.[260] This is consistent with the general legal framing of Data Protection compliance as an obligation or condition of doing business. Responsibility to honor erasure requests exists independently of any liability in the sense of exposure to civil tort claims[261] or monetary damages.[262] If the eCommerce Intermediary

---

[257] As Ausloos and Kuczerawy put it,

> the ruling does not impose search engine liability over the (publication of the) original content. Instead, the scope of application is concentrated on the search engine's activity of linking a specific search term (name of an individual) with a specific search result. This operation, after all, is entirely within the hands of the search engine.

Ausloos and Kuczerawy, *supra* note 3, at 7.

[258] By this reasoning, the EU eCommerce Directive arguably would not protect OSPs from direct liability for claims such as defamation or copyright, but only from secondary liability arising from users' actions. This would seem to defeat the purpose of the Directive's safe harbors, rendering OSPs liable for content they knew nothing about. *See* Opinion of Advocate General Szpunar, *supra* note 59, at para. 64 (EU eCommerce Directive shields OSPs from "direct liability and secondary liability for acts committed by third parties").

[259] *See* discussion of *Google Spain*, *supra* note 2, at para. 82-88.

[260] GDPR R. 74, 79, 80.

[261] *See Article 29 Search Engine Opinion*, *supra* note 80 at p. 14. (search engine Controller status for processing website content is "separate from the issue of liability for such processing").

[262] The GDPR generally uses to term "liability" in reference to financial damages to data subjects. *See e.g.*, GDPR R. 74, R. 146 (allocation of liability between processors and controllers), Art. 47(2)(f) (same), Art. 82 ("Right to compensation and liability" – damages to individuals harmed by data processing)

Liability framework applied only to liability under one of these narrow definitions, it might be inapplicable to RTBF as a doctrinal matter.

But applicability of the eCommerce Rules does not depend on the doctrinal basis of an OSP's removal obligations. They are relevant for any claim that holds OSPs responsible for information posted by a user, applying, as Advocate General Szpunar has said, to "all forms of liability for unlawful acts of any kind, and thus to liability under criminal law, administrative law and civil law, and also to direct liability and secondary liability for acts committed by third parties."[263] They address both monetary damages and injunctive relief, prohibiting the former and limiting the scope of the latter.[264] They even apply – and limit the obligations that may be placed on OSPs – when an OSP has no liability at all under Member State law.[265] So, for purposes of determining whether eCommerce Rules apply to RTBF, it does not matter whether RTBF obligations are considered a form of liability, or are rooted in some other legal doctrine.

From the perspective of fundamental rights, too, these questions are largely semantic. A person whose expression is erased or de-listed suffers the same harm – and state action plays the same role in creating that harm – regardless of what law prompted the OSP to do it. What matters to the affected user is that a private actor, operating under actual or perceived legal compulsion, erased her expression without telling her or giving her an

---

[263] Opinion of Advocate General Szpunar, *supra* note 59, at para. 64.

[264] EU eCommerce Directive Art.15; SABAM, 2011 E.C.R. (rejecting over-broad injunctions under Article 15). The eCommerce immunity provisions also address liability beyond monetary damages. *See* EU eCommerce Directive 14.1(a) (distinguishing constructive knowledge standard for damages from actual knowledge standard for other forms of liability); L'Oreal, 609CJ0324, para. 119.

[265] *See* Husovec, *supra* note 44, at 116-118; L'Oreal, 609CJ0324 at para. 127 (approving injunction against intermediary "regardless of any liability of its own" under Directive 2004/48/EC) and 139 (requiring that said injunction comply with eCommerce Directive prohibition on general monitoring obligations). *See also* Report from the Commission to the Council, the European Parliament and the European Social Committee on the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights COM (2010) at 17, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010SC1589 (injunctive relief "granted against the intermediary irrespective whether there has been a determination of liability of the intermediary" is not barred by EU eCommerce Directive). Further research on the uses of the term "liability" in the Intermediary Liability context would be instructive.

opportunity to object. The procedural protections of Intermediary Liability law exist to address this problem.

2. Confusing Language in the Governing Instruments

Uncertainty about whether eCommerce Rules should apply to RTBF as a principled matter is compounded by unclear prescriptions in the written law. The GDPR has language that might -- or might not – resolve the entire issue by expressly invoking the eCommerce Rules for RTBF notice-and-takedown. Meanwhile, the eCommerce Directive contains language that might or might not prevent that law from applying to Data Protection claims in the first place. Both provisions are open to either reading – but, based on considerations of fundamental rights, they should be interpreted apply eCommerce Rules to RTBF.

a) Language in the eCommerce Directive

The eCommerce Directive contains a passage, in Article 5.1(b), that is widely interpreted as carving out Data Protection issues from its scope. It says that the eCommerce Directive "shall not apply to… questions relating to information society services covered by" Data Protection law, including the GDPR.[266] Following one interpretation, this would mean that eCommerce Rules do not apply to notice-and-takedown requests that are based

[266] EU eCommerce Directive Art. 5.1(b); *see also* GDPR Art. 94 GDPR ("References to the repealed Directive shall be construed as references to this Regulation.") An EU eCommerce Directive recital suggests that the Intermediary Liability rules do apply, and must merely be interpreted consistently with Data Protection: "the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards … the liability of intermediaries." EU eCommerce Directive R.14. But it also includes language that could indicate the opposite – that Data Protection law simply displaces eCommerce Rules.

> The protection of individuals with regard to the processing of personal data is solely governed by [laws including the 1995 Directive], which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive.

on Data Protection claims – including RTBF requests. In my experience, this reading of Article 5.1(b) is conventional wisdom among many European practitioners.

In a 2016 ruling, an Northern Irish appeals court rejected this interpretation, however. In a case against Facebook, it concluded that Intermediary Liability is *not* one of the "questions … covered by" the 1995 Directive.[267] The eCommerce Rules apply to notice-and-takedown claims based on Data Protection, it said, as those rules "do not interfere with any of the principles in relation to the processing of personal data[.]"[268] This interpretation is compelling: it makes sense of the language, harmonizes the two sources of law, and preserves balance among affected fundamental rights. It will likely be contested, however, in future cases.

b) Language in the GDPR

The GDPR invokes the eCommerce Rules directly in Article 2.4, saying

> This Regulation shall be without prejudice to the application of [the eCommerce Directive], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.[269]

At first glance, this seems to expressly apply eCommerce Rules to RTBF. But the meaning of the passage depends whether the eCommerce "liability rules of intermediary service providers" cover Data Protection notice-and-takedown in the first place. In other words, it depends on one's interpretation of eCommerce Directive Article 5.1(b), discussed above. If the eCommerce Rules do not, by their own terms, apply, then the

---

[267] Facebook Ireland, (2016) NICA.

[268] *Id*. at 30-31. Arguably the outcome of this analysis should be different under the GDPR, on the theory that notice-and-takedown procedures *are* a "question… covered by" that law – even though they are not covered in the 1995 Directive. This analysis is complicated by language in the GDPR itself, discussed in the next section, that seemingly applies the EU eCommerce Directive to its own proceedings.

[269] GDPR Art. 2.4. *See also* R. 21 ("This Regulation is without prejudice to the application of [the EU eCommerce Directive] in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.")

GDPR could be "without prejudice" to eCommerce Rules simply because each law covers a different set of questions.

That said, if the GDPR drafters were trying to say "these are two unrelated laws," the passage at Article 2.4 quoted above would be an odd way to say it. The more natural interpretation is the simpler one: that the GDPR invokes eCommerce Rules for RTBF notice-and-takedown – and, implicitly, rejects the idea that ordinary Intermediary Liability law under the eCommerce Directive does not reach RTBF notice-and-takedown. Following this interpretation, the GDPR Rules would remain important and effective for erasure requests that target stored, back-end data. But public, online expression would get the more robust protections of the eCommerce Rules.

3. Reconciling the eCommerce Directive and Data Protection Law

One major ruling to date has made a serious effort to reconcile OSPs' obligations under European Intermediary Liability and Data Protection laws. In a case raising Data Protection claims about a video hosted by Google, Italy's highest court held that eCommerce Rules applied.[270] As a result, Google was not legally responsible for the video – which depicted bullying– prior to the time when Google was notified about it and took it down. The Italian court said that Article 5.1(b) of the eCommerce Directive, "does not have the purpose to render the eCommerce provisions inapplicable to any case concerning the protection of personal data."[271]

According to the court, the eCommerce and Data Protection frameworks can be reconciled by holding that in general the user who posts content, and not the OSP that hosts it, is its Controller. The OSP becomes a Controller, however, once it is notified about user content that violates Data Protection law:

---

[270] Cass. sex. III Penale, 3 febbraio 2014, n. 5107/14, Milan Public Prosecutor's Office v. Drummond, http://www.dirittoegiustizia.it/allegati/15/0000063913/Corte_di_Cassazione_sez_III_Penale_sentenza_n_5107_14_depositata_il_3_febbraio.html (informal translation).

[271] *Id.* at para. 7.4.

> [A]s long as the service provider is not aware of the unlawful data, the service provider cannot be considered to be the data controller since the provider does not have any decision-making power over the data; on the other hand, if the provider is aware of the unlawful data, and does not do something to immediately remove it or make it inaccessible, the provider then fully takes on the status of data controller, and is therefore subject to the duties and criminal sanctions of [Data Protection law].[272]

This theory, that only OSPs with knowledge are Controllers, has some benefits. Importantly, it relieves OSPs of Controller obligations in the time before receiving removal requests. As discussed in Section II.C, classifying OSPs as Controllers of every bit of automatically-processed user expression would subject them to illogical or impossible obligations. The Italian court's bright-line rule creates a relatively high degree of legal certainty for OSPs trying to understand their obligations under Data Protection law. In that sense it is better than *Google Spain*'s hazier standard: that a search engine is a Controller, but its obligations are limited to "ensur[ing], within the framework of its responsibilities, powers and capabilities" that it complies with Data Protection law.[273]

Whatever the merits of this framing, however, it does not solve the procedural notice-and-takedown problems created by the GDPR. If an OSP becomes a Controller in the moment of receiving a removal request, it still must decide what notice-and-takedown rules to follow: eCommerce Rules, or GDPR Rules. The choice has real consequences for the rights of Internet users.

There is another, superficially plausible, variant on the Italian Court's approach that raises still more problems. It could be argued that Controllers never fall within the

---

[272] *Id.* at para. 7.2. In another dispute raising the issue in 2015, a UK court stated a "provisional preference" for the conclusion that "the two Directives must be read in harmony and both, where possible, must be given full effect to." Mosley v. Google, [2015] EWHC (QB) 59 (describing but not resolving question whether eCommerce Rules apply to Data Protection claims). The case, which this author worked on as counsel to Google, concerned plaintiff's request for Google to proactively filter images from web search results, based on Privacy and Data Protection rights.

[273] *Google Spain, supra* note 2, at Par. 38, emphasis added.

eCommerce safe harbors, because in determining the "purposes and means" of processing user-generated content, they take too active a role to qualify for immunity under the Directive. Conflating the Data Protection and eCommerce classifications in this manner would in theory align the two frameworks as follows:

Data Processors under 1995 Directive or GDPR	=	Immunized "passive" OSPs under eCommerce Directive
Data Controllers under 1995 Directive or GDPR	=	Non-immunized "active" OSPs under eCommerce Directive

This equation has troubling consequences for both areas of law, though. For one thing, it would strip OSPs of Intermediary Liability protection for claims entirely unrelated to Data Protection. Following this theory, *Google Spain*'s holding that Google is a Controller would take away its eCommerce Directive defenses for copyright claims, defamation claims, and much more. This would not only be bad policy, it would conflict with cases and laws establishing Intermediary Liability protections for search engines.[274]

Similarly, Data Protection rules need to cover a vast array of issues unrelated to notice-and-takedown, from employer record-keeping to online targeted advertising. Court rulings in eCommerce cases about unrelated issues – like trademark claims or hate speech – should not have the unintended consequence of distorting Data Protection regulation. The eCommerce active/passive distinction and Data Protection's Controller/Processor distinction are themselves moving targets within two separate, complex, and rapidly changing legal fields. The evolution of the two bodies of law should not be distorted by hitching their key classifications together.

Finally, conflating the two classification systems would not address the problems with RTBF notice-and-takedown. It would put the very OSPs that must honor RTBF requests

[274] *See* cases listed *supra* n. 46.

– Controllers -- outside of the eCommerce Directive's Intermediary Liability framework, and effectively strip Internet users of key legal protections against over-reaching RTBF removal demands.

V. SOLUTIONS

Throughout this Article, I have detailed unnecessary risks of the GDPR's notice-and-takedown provisions, and suggested legal arguments to mitigate them. This final Section briefly distills those arguments into specific proposed solutions.

The most immediate avenue for improving the GDPR is through actions of the new Board or Member State legislators. Both will have critical opportunities to shape real-world OSP behavior through laws and guidelines they publish. Member States, which are mandated to pass laws balancing free expression with the new GDPR rights, can enact important limitations within their own jurisdictions. The Board can issue and refine EU-wide guidelines for DPAs, OSPs, and data subjects who send RTBF requests. In consultation with EU Intermediary Liability and free expression rights experts, both could arrive at well-crafted, balanced approaches.

A second means of improving GDPR notice-and-takedown is through disputes and litigation before DPAs or courts. This approach would likely lead at best to piecemeal resolution of the problems described here. But, for problems that are not addressed by Board or Member State action, it is likely the best remaining option.

A. Rules from the eCommerce Directive Should Govern Notice-and-Takedown under the GDPR

This Article argues that the notice-and-takedown regime described in the GDPR lacks the procedural tools to adequately protect expression rights, and that the eCommerce Directive is a better source of law for RTBF requests targeting public, online

information.[275] Adopting rules based on the eCommerce Directive would be the simplest solution to an array of problems identified in Section III.C of this Article. The Board's notice-and-takedown guidelines could easily track the protections of the eCommerce Directive, and even offer improvements over Member States' current implementations.[276] Article 2.4 of the GDPR provides a simple legal basis for doing so.[277] That would leave the GDPR's provisions intact and effective for erasure of back-end, privately held data such as user accounts or ad-targeting profiles.

B. If GDPR Rules Apply to Notice-and-Takedown, They Should Be Interpreted to Maximize Procedural Fairness

If lawmakers do not invoke eCommerce Rules for erasure of public online content, the next best hope is to interpret GDPR Rules in a way that restores a measure of balance between the different fundamental rights affected by notice-and-takedown of online information. Interpretations along these lines are discussed in Section III of this Article. For example, lawmakers could determine that requests to temporarily "restrict" access to online data while an OSP reviews a data subject's erasure request do not apply to online expression, or apply only in narrowly defined cases.[278] The challenge with this approach arises from reliance on potentially strained interpretations of GDPR text. For example, it is hard to come up with alternate interpretations of provisions that seem require OSPs to disclose personal data about online speakers.[279] Without the clean sweep displacement of GDPR rules by eCommerce rules, protection for online speakers would be limited by each individual problematic GDPR provision.

---

[275] *See* discussion *supra* Section III.B, IV.A.

[276] *See Commission Staff Working Document, e-Commerce action plan 2012-2015,* EUROPEAN COMMISSION (2012), http://ec.europa.eu/internal_market/e-commerce/docs/communications/130423_report-ecommerce-action-plan_en.pdf at 44 (identifying issues and areas for improvement in eCommerce notice-and-takedown procedures).

[277] *See* discussion *supra* Section IV.B.2.b.

[278] *See* discussion *supra* Section III.C.2.

[279] *See* discussion *supra* Section III.C.6.

C. Hosts Should Not Be Subject to RTBF Obligations.

Excluding hosting services from obligations to erase users online expression would mitigate one of the greatest potential threats to information rights under the GDPR. As discussed in Section III.B, governing law on this topic is extremely open to interpretation. Hosts, including social media services, could be Controllers, or not. The reasoning of *Google Spain* could apply to them in part or not at all. Regardless of how these questions are resolved, hosts will continue to have removal obligations for other claims, including defamation and privacy torts.

If hosts did have to remove content based on RTBF claims, they clearly would need to follow different rules than the ones applied to search engines. New guidance would be required both for hosts' substantive standards in weighing the public interest against RTBF requests, and their technical implementation for honoring them.

Uncertainty about hosts and RTBF creates particularly strong risks of over-removal, because of hosts' incentives to avoid disputes that could lead to them being classified as Controllers. A clear message that hosts will not be held to RTBF obligations, even if temporarily, could minimize this threat to Internet users' expression and information rights.

D. DPAs Should Not Assess Financial Penalties Against OSPs That Reject RTBF Requests in Good Faith.

Fear of high fines gives OSPs reason to readily remove user-generated content, even if the request for removal is over-reaching and unsupported by European law. The problems of combining perceived or real financial pressure with unclear RTBF rules are discussed in Section III.A. Lawmakers could protect ordinary Internet users and bring OSPs' incentives into better balance by assuring OSPs, clearly and in writing, that they do not risk fines when they reject questionable RTBF requests or preserve procedural notice-and-takedown protections for their users.

Such an assurance would not turn indifferent OSPs into defenders of users' rights, since standing up for them would still impose costs in time, lawyers' fees, or exposure to regulatory attention. But for those with limited resources and some desire to protect users, it could make a very important difference.

E. EU Member State Law and Regulatory Guidance Should Robustly Protect Freedom of Expression in RTBF Cases

The GDPR expressly charges Member States with protecting free expression, and mandates that DPAs broadly protect fundamental rights and freedoms of all sorts.[280] On this basis, either or both could establish thoughtful substantive standards to guide OSPs considering which RTBF requests to honor. Such standards will be particularly important for hosts, if they are deemed Controllers, since existing guidance for search engines is inappropriate for them and would lead to over-removal.[281] Free expression rights can also be protected through procedural rules discussed throughout this Article.

F. National Legal Differences Should Be Respected

The GDPR risks creating a systematic imbalance by making Data Protection rights "exportable" to require extraterritorial deletion of content, while free expression rights apply only locally at best – or at worst are globally over-ridden by the most conservative national Data Protection laws. The jurisdiction and choice of law rules governing Data Protection claims are complex. But they can and should be resolved to balance all affected rights of Internet users, as well as the interests of national governments both within and outside of the EU. As discussed in Section III.E, the answer should not simply be that countries requiring erasure always prevail over those that do not.

---

[280] GDPR Art. 51.1 (DPA Mandate).

[281] *See* discussion *supra* Section III.C, III.B.3,

VI. CONCLUSION

Privacy and information rights are in principle equally important, and protected proportionally under EU law. Balance between the two rights is necessary to support individual liberty and democratic participation.

The GDPR unintentionally but seriously disrupts this balance, tilting the playing field in favor of privacy rights and the individuals who assert them. It does so through seemingly innocuous procedural rules for data Controllers – rules which, when applied to OSPs' notice-and-takedown systems for public online speech, systematically favor erasure.

The result is a powerful new tool for abusive claimants to hide information from the public. Bloggers documenting misuse of power can be silenced, and small businesses can lose access to customers, all through secret accusations sent to private technology companies. Beyond the realm of deliberate misuse, for RTBF claims that raise genuinely hard-to-resolve questions about Data Protection and the public interest, the GDPR's rules systematically push toward removing or de-listing information. As few of these decisions will ever reach public adjudication, the de facto rules governing a vast swath of online expression will be defined by OSP practice under the GDPR.

The good news is that much of this harm can be avoided – and avoided without sacrificing the Data Protection and privacy rights safeguarded by the GDPR. Existing law under the eCommerce Directive and the EU's fundamental rights framework provides the tools. We should all hope lawmakers use them.