Stanford Law School
Law and Policy Lab

Intermediary Liability & Human Rights Policy Practicum

The "Right to Be Forgotten" and Blocking Orders under the American Convention: Emerging Issues in Intermediary Liability and Human Rights

2017 PRACTICUM RESEARCH TEAM:

Subhajit Banerji, Savni Dutt, Ella Hallwass, Yindee Limpives, Miguel Morachimo, and Mirena Taskova. LL.M. Candidates June 2017
Shelli Gimelstein and Shane Seppinni. J.D. Candidates 2018

LEAD STUDENT EDITOR:

Savni Dutt. LL.M. Candidate June 2017

INSTRUCTORS AND PROJECT LEADS:

DAPHNE KELLER
Lecturer in Law
Director of Intermediary Liability, Center for Internet and Society

LUIZ FERNANDO MARREY MONCAU
Intermediary Liability Fellow, Center for Internet and Society, Stanford Law School

CLIENT:

Office of the Special Rapporteur for Freedom of Expression, Organization of American States

September 2017

Acknowledgements

This report is based on the research and work of participants in Stanford Law School's Intermediary Liability and Human Rights Policy Lab Practicum (Winter / Spring 2017).

The work also reflects guidance and input from scholars and experts. We would like to thank Mark Lemley for his insightful input, Lea Shaver and Alex Zhang for important guidance on international human rights research, Luciana Herman for her extensive oversight and input on methodology, and Jeremy Malcolm and the Electronic Frontier Foundation for vital guidance and conversations about intermediary liability, in general, and the Manila Principles on Intermediary Liability, specifically. We would also like to thank the LL.M Candidate (June 2017) Clarisse Medeiros de La Cerda for the inputs, participation and research as an auditing student of the Policy Practicum.

Additionally, we would also like to acknowledge the important support of people and departments at Stanford Law School, including Sergio Stone, deputy director of the Robert Crown Law Library, and Phillip Malone and Jef Pearlman of the Juelsgaard Innovation and Intellectual Property Clinic.

Finally, we are extremely thankful for the opportunity to collaborate with the Office of the Special Rapporteur for Freedom of Expression at the Organization of American States, and to Mr. Edison Lanza for his directions, recommendations, and ideas in drafting this report.

About the Stanford Law School Policy Lab

Engagement in public policy is a core mission of teaching and research at Stanford Law School. The Law and Policy Lab (The Policy Lab) offers students an immersive experience in finding solutions to some of the world's most pressing issues. Under the guidance of seasoned faculty advisers, Law and Policy Lab students counsel real-world clients in an array of areas, including education, intellectual property, public enterprises in developing countries, policing and technology, and energy policy.

Policy labs address policy problems for real clients, using analytic approaches that supplement traditional legal analysis. The clients may be local, state or federal public agencies or officials, or private non-profit entities such as NGOs and foundations. Typically, policy labs assist clients in deciding whether and how qualitative or quantitative empirical evidence can be brought to bear to better understand the nature or magnitude of their particular policy problem, and identify and assess policy options. The methods may include comparative case studies, population surveys, stakeholder interviews, experimental methods, program evaluation or big data science, and a mix of qualitative and quantitative analysis. Faculty and students may apply theoretical perspectives from cognitive and social psychology, decision theory, economics, organizational behavior, political science or other behavioral science disciplines. The resulting deliverables reflect the needs of the client with most resulting in an oral or written policy briefing for key decision-makers.

Directed by former SLS Dean Paul Brest, the Law and Policy Lab reflects the school's belief that

systematic examination of societal problems, informed by rigorous data analysis, can generate solutions to society's most challenging public problems. In addition to policy analysis, students hone the communications skills needed to translate their findings into actionable measures for policy leaders and the communities they serve. The projects emphasize teamwork and collaboration, and many are interdisciplinary, giving law students the opportunity to work with faculty and colleagues from across the university with expertise in such fields as technology, environmental engineering, medicine, and international diplomacy, among others.

About the Center for Internet and Society

The Center for Internet and Society (CIS) is a public interest technology law and policy program and a part of Law, Science and Technology Program at Stanford Law School. CIS brings together scholars, academics, legislators, students, programmers, security researchers, and scientists to study the interaction of new technologies and the law and to examine how the synergy between the two can either promote or harm public goods like free speech, innovation, privacy, public commons, diversity, and scientific inquiry. CIS strives to improve both technology and law, encouraging decision makers to design both as a means to further democratic values. CIS provides law students and the general public with educational resources and analyses of policy issues arising at the intersection of law, technology and the public interest. The Center is directed by Stanford Law Professor Barbara van Schewick.

TABLE OF CONTENTS

PART I: EXECUTIVE SUMMARY

Today, an increasing number of social and economic activities depend on the internet and the internet functions through intermediaries at every stage. The internet has increasingly become the critical platform for all types of speech: news, comments, opinions, political organization, and more. Internet intermediaries host, index, and provide access to this speech and, hence, play an important role in facilitating free expression on the internet. This Report considers the nature and scope of liability imposed on intermediaries for speech shared online by internet users, and the ways that such liability may indirectly lead to suppression of lawful speech. By reviewing key human rights documents from the OAS and other international systems, it identifies core substantive and procedural norms that must shape intermediary liability in order to protect users' rights to free expression. It then considers two recent trends that are gaining traction around the world: the so-called 'right to be forgotten doctrine' ('RTBF') and orders compelling Internet Service Providers ('ISPs') to block entire websites, applications or services ('site and service blocking' or 'SSB'). Both issues are understood through existing jurisprudence, international human rights documents and sources specific to the OAS countries.

The objective of this Report is to provide the Office of the Special Rapporteur on the Freedom of Expression ('OSRFE') for the OAS countries with an overview of human rights considerations raised by RTBF and SSB. This resource can then be used by the OSRFE to understand the treatment of these issues within OAS countries and especially, to identify: (a) whether the emerging trends are acceptable under the OAS human rights framework; (b) countries within the OAS that are complying with the OAS human rights framework with their treatment of RTBF and SSB, and; (c) problem areas within the OAS region that need the Special Rapporteur's attention and suggestions.

It is important to consider and study the emergence of RTBF and SSB because these issues are currently in the developing stage, with opportunities to advocate for approaches and interpretations that respect free expression rights. It is also noticeable that while the OAS human rights framework is uniquely protective of expressive freedoms, individual OAS countries have very different ways of interpreting laws that affect free expression. For instance, some mirroring may be observed of the European developments, particularly with respect to RTBF and data protection laws, in OAS states. As such, this is a critical time to attend to these issues and preserve strong protections for freedom of expression in the OAS countries. To that end, this Report aims to provide a helpful source of information for the OSRFE.

As interpreted by authoritative sources, the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights call for equal human rights online and offline. In the OAS human rights framework, the American Convention on Human Rights ('ACHR') lays down the guiding principles. Most importantly, Article 13 of the ACHR provides the three-step test for all actions that may restrict the freedom of expression. The ACHR's unique prohibition on laws that restrict expression by "indirect methods" including "government or private controls over ... equipment used in the dissemination of information" provides an unusually clear mandate that laws governing Internet intermediaries must not effectively suppress free expression. Regional human rights sources and interpretations confirm this, repeatedly urging clear

intermediary liability principles to avoid removal of lawful speech. Guidelines drawing on OAS and other international human rights sources have been collected and detailed in a key civil society document, the Manila Principles.

Procedurally, both OAS sources and the Manila Principles emphasize the importance of adjudication by an independent judicial body before intermediaries are legally obliged to remove users' expression. Additionally, there is also importance given to the right of an affected person to be informed of a restriction and given a chance to redress their grievance. Concerning the intermediaries, there is also an emphasis on the transparency of policies and practices of an intermediary.

Both RTBF and SSB developments may be in considerable tension with -- or simply in violation of -- OAS free expression standards, particularly as those standards relate to intermediary liability.

The so-called 'right to be forgotten' doctrine rose to prominence following the European Court of Justice's 2014 *Google Spain* decision, and has generated a significant trend of similar claims within OAS countries. Particularly in countries with data protection laws modeled on the EU's, some have supported following the *Google Spain* model: designating search engines as data controllers, and compelling them to de-list links to webpages containing personal information upon request. Judicial acceptance of this argument has varied within OAS countries. At least two important cases have highlighted points of tension between RTBF and regional or national protections for free expression rights. A Colombian court identified net neutrality and free expression concerns as reasons not to impose RTBF obligations on a search engine, but did require a news publisher to exclude pages from Google's search index. A Mexican court, in a key case vindicating procedural rights, rejected an RTBF order against the search engine because the publisher of the web page at issue had not been notified of the order or given an opportunity to contest it. In Peru, by contrast, Google was compelled to de-list webpages on RTBF grounds. This diversity of interpretations indicates an important opportunity for guidance from the OSRFE on whether or how the EU model can be reconciled with the OAS human rights framework.

Similarly, there have been several instances of SSB in the OAS countries. ISPs have been compelled to block entire websites and, more famously, popular applications like Whatsapp and Uber. However, there is no uniformity in the laws applied. Some countries in the OAS that do not have specific laws concerning SSB have used other existing laws to justify their imposition. As with RTBF, any restriction that limits the freedom of expression must comply with the three-part test, and in particular must be narrowly tailored and accompanied by procedural protections against over breadth. SSB orders that compel ISPs to block entire websites when only some pages are known to contain unlawful content are highly unlikely to meet these standards. In order to comply with OAS human rights standards, courts and government actors should consider and exhaust less restrictive approaches, such as blocking individual pages or requesting that the website remove content, before resorting to SSB orders against ISPs. Even when states have particularly compelling grounds to restrict content, such as to combat child pornography, procedural protections against over-blocking are critical. These may include notice to the affected website or application provider; notice to affected users seeking the site or service; opportunities to contest

blocks; geographic and temporal limits on the scope of blocking orders; and broad public transparency about government and ISP blocking practices.

Apart from the inherent conflict of SSB orders with freedom of expression, SSB also conflicts with the principle of network neutrality. A number of countries including Canada, Colombia and Chile have seen recent attention in their legislation to promoting network neutrality, suggesting that it, along with core intermediary liability principles, provides an important limit on SSB orders to block online expression.

Drawing on our review of human rights documents and emerging trends globally and within OAS countries, this Report proposes the following actions by the OSRFE. These are discussed in more detail within each of the substantive parts of this Report, with specific proposals for RTBF and SSB.

a. Sending information requests regarding the existing regulations concerning intermediaries in the OAS.
b. Recommending the incorporation of free expression review, and the involvement of experts specialized in free expression, in any proceedings regarding RTBF or SSB.
c. Preparing special reports with interpretative principles to guide RTBF and SSB interpretation, and inviting the countries to study the effectiveness of their existing regimes.
d. Assisting in the development of the meaning of 'least restrictive means' in the SSB context, and thereafter formulating possible interventions between the least and most restrictive measures.
e. Assisting in the development of guidance for agencies and courts interpreting data protection laws in cases affecting free expression.
f. Promoting and calling upon member states to promote transparency regarding removal orders or requests to intermediaries.
g. Encouraging multi-stakeholder discussions between intermediaries, civil society, and governments to discuss existing measures and propose new measures that would limit intermediary liability and at the same time increase understanding of the limits of intermediary responsibility.

PART II: GENERAL REPORT INTRODUCTION

A. Introduction

If anyone ever doubted the reach and importance of internet intermediaries, the past five years should have put these doubts to rest. In the height of the refugee crisis in Syria, Facebook, Twitter, WhatsApp and Viber arose as tools protecting human life.[1] With the Internet's bountiful growth and its integration into daily life, Internet regimes no longer affect merely work and entertainment but now have a direct impact on human rights and public policy. Internet actors – specifically intermediaries – have risen to prominence to become leading points of access to information and primary modes of communication and expression.[2]

Internet intermediaries include, but are not limited to, social media networks, search engines, online marketplaces and Internet service providers ('ISPs'). This report examines the liability of intermediaries globally and especially in the countries of the Inter-American system as part of the Organization of American States ('OAS countries'). It focuses on the impact of such regulation on freedom of expression and other intersecting human rights online. Intermediary liability laws that impact free expression bear particular scrutiny in the OAS countries, because of the Inter-American System's recognized status as the international framework that secures the broadest protections for the right to freedom of thought and expression.[3]

Intermediaries are often treated as the 'gatekeepers' to the internet,[4] because they may have the technical capability to control and even block Internet users' access to particular content. As a result, intermediaries are sometimes held legally responsible for removing or blocking content generated by third parties, such as independent webmasters or social media users. Two important intermediary liability developments are examined in this report: orders compelling intermediaries to block entire websites or services, and obligations for intermediaries to remove or de-list content under the doctrine known as the "right to be forgotten."

This report analyses over 25 human rights documents and finds a recurring emphasis on strictly limited removal obligations for intermediaries. The documents reviewed were issued by international bodies such as the United Nations and the Inter-American Commission on Human Rights ('IACHR'), advocacy groups such as Article 19, and multi-stakeholder initiatives like the Manila Principles and the Global Network Initiative. The analyzed documents include international agreements that protect human rights worldwide and within the OAS system, as well

---

[1] Mathew Brunwasser, *A 21st-Century Migrant's Essentials: Food, Shelter, Smartphone*, N.Y. Times, (Aug. 25, 2015) https://www.nytimes.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html?_r=2 [https://perma.cc/NE4Q-YKUR].

[2] Pew Research Center U.S. Policy & Politics, *Internet Overtakes Newspapers as News Outlet*, (Dec.23, 2008), http://www.people-press.org/2008/12/23/internet-overtakes-newspapers-as-news-outlet/ [https://perma.cc/99WD-RXZR].

[3] IACHR OSRFE, *The Inter-American Legal Framework regarding the Right to Freedom of Expression* (2010) 14, http://www.oas.org/en/iachr/expression/docs/publications/INTER-AMERICAN%20LEGAL%20FRAMEWORK%20OF%20THE%20RIGHT%20TO%20FREEDOM%20OF%20EXPRESSION%20FINAL%20PORTADA.pdf [https://perma.cc/5865-XMS4].

[4] Article 19, Internet Intermediaries: Dilemma of Liability, (London, 2013) https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf [https://perma.cc/TD4N-GS93].

as materials interpreting core protections for free expression and other human rights in the context of intermediary liability. The report then undertakes a broad, but by no means exhaustive, overview of emerging trends in "Right to Be Forgotten" ('RTBF') and site and service blocking ('SSB') laws in OAS states, and analyzes these developments in light of the applicable human rights standards with a focus on rights to free expression.

B. What Is Intermediary Liability?

The OECD defines internet intermediaries as those who "give access to, host, transmit and index content originated by third parties or provide Internet-based services to third parties."[5] Internet intermediaries are distinct from "content providers," which are "those individuals or organizations who are responsible for producing information in the first place and posting it online."[6] There are several types of intermediaries, including internet/network service providers, domain name registrars, web-hosting services, search engines, e-commerce platforms, social media companies, and participative networking platforms.[7] There are some intermediaries that do not fall within a single category and instead offer multiple services.

Intermediary Liability laws define the scope and extent of responsibility that may be imposed on an intermediary for content shared by internet users. Regulation of the internet content may arise from diverse legal doctrines, including defamation, blasphemy, hate speech, intellectual property rights, obscenity, public order, national security, child protection, and more.[8] Intermediaries are also sometimes penalized or compelled to block content based on legal claims unrelated to speech and expression -- for example, based on data localization requirements.[9] While some of these regulations may be necessary to protect essential public interests and even to protect other human rights including rights to privacy,[10] poorly considered application of these laws to intermediaries affects ordinary Internet users' ability to seek and impart information, and can violate the free expression obligations of state actors.[11]

Different approaches to intermediary liability have distinguishable consequences for

---

[5] OECD, *The Economic and Social Role of Internet Intermediaries*, (Apr. 2010) https://www.oecd.org/internet/ieconomy/44949023.pdf [https://perma.cc/M73H-KR3V] at 4.

[6] Article 19, (2013) *supra* note 4 at 6.

[7] David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (UN) , A/HRC/32/38, 11 May 2016 at 6-8, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/38 [https://perma.cc/9MN8-Y86D]; Rebecca Mackinnon et al, Fostering Freedom Online the Role of Internet Intermediaries (2014), UNESCO Publishing, http://unesdoc.unesco.org/images/0023/002311/231162e.pdf [https://perma.cc/J6LX-7K68], 21.

[8] A/HRC/32/38 (2016).

[9] *LinkedIn Blocked by Russian Authorities*, BBC, (Nov. 17, 2016) http://www.bbc.com/news/technology-38014501 [https://perma.cc/8QF2-TUYV].

[10] Examined under the analysis of Article 13 para 3 in Part III and IV.

[11] Other relevant rights that impact intermediaries include, but are not limited to, due process rights, non-discrimination in access to the internet, right to privacy, and net neutrality. Parts III and IV of the Report will consider these issues as they arise in connection to freedom of expression and right to access online, but does not delve into a detailed analysis of intermediary liability in these areas.

freedom of expression. Potential liability regimes for intermediaries may be roughly divided into three categories: strict liability, complete immunity and safe harbor or notice-based liability.[12] A strict liability regime would impose unconditional liability on the intermediary for the illegality of content uploaded by third parties and would de facto require the intermediary to police content that is posted on their service in order to avoid liability.[13] At the other extreme, complete immunity allows intermediaries to continue hosting, transmitting, or otherwise processing even information that has been adjudicated as violating the law.

As a middle ground between these two approaches, many countries provide safe harbors to intermediaries.[14] Such safe harbors create conditional immunity for the intermediary, typically establishing obligations or potential liability only once an intermediary gains knowledge of unlawful content. This immunity is often subject to conditions such as that the intermediary must not interfere in the selection or the transmission of user content to specific audiences. The immunity may also be limited based on timely action by the intermediary for the removal of content once it learns of the unlawful content, as prescribed by the local laws.[15] Under such "notice and takedown" regimes, removal obligations may arise based on requests made by governments, requests from private entities, orders from courts, or the intermediary's own discovery of unlawful content.

This Section will discuss these three approaches to intermediary liability in more detail.

1. Complete Immunity Approach

There are relatively few legislative examples of the complete immunity approach. One such example is the U.S. Communications Decency Act, 1996,[16] which immunizes users and providers of interactive internet services from liability for most claims regarding content produced by another. Supporters of this approach point out that it maximizes commercial incentives to create online speech platforms, and that it avoids the significant risk of platforms being overly cautious and removing lawful content for fear of liability. Detractors note that it permits content that has been adjudicated as unlawful and harmful, such as defamation, to remain widely available online.

2. The Safe Harbor Approach

Safe harbor intermediary liability laws condition the platform's immunity on its compliance with specific responsibilities. A common model is "notice and takedown," but other important variants are "notice and notice" or "judicial notice" models.

---

[12] *See generally* Article 19, (2013) *supra* note 4.

[13] OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, (June 22, 2011) at 32 http://www.oecd.org/internet/ieconomy/48685066.pdf [https://perma.cc/7VDA-EVEB]..

[14] *See* discussion *infra* Part I.A.5.

[15] Information Technology (Intermediaries Guidelines) Rules, 2011 , World Intermediary Liability Lab: India, http://cyberlaw.stanford.edu/page/wilmap-india [https://perma.cc/M3AP-FS5F]; the Chilean provision provides that effective knowledge of an intermediary means knowledge by means of a court order, World Intermediary Liability Map: Chile, http://cyberlaw.stanford.edu/page/wilmap-chile [https://perma.cc/PV3A-N4EK].

[16] 47 U.S.C. s. 230(c)

Under "notice and takedown" systems, intermediaries respond to valid notices of unlawful content by removing the content. One of the most procedurally detailed regulatory frameworks in intermediary laws is the 'notice and takedown' system provided under section 512 of the U.S. Digital Millennium Copyright Act ('DMCA').[17] The DMCA legislation enumerates the specific information that a complainant must submit to an intermediary for the removal of a content, and preserves intermediaries' immunity if they receive notices that do not provide the specified information. The DMCA also incentivizes the intermediary to inform the alleged copyright infringer when content has been removed, and give that person the opportunity to submit a "counter-notice" refuting the allegation of infringement. The intermediary can then reinstate the content without risk of liability, and leave it up until such time as the right holder brings its claims to court.[18] Despite these relatively robust procedural protections, empirical studies show that intermediaries frequently remove lawful content in response to over-reaching DMCA requests, and that the counter-notice process does little to correct this.[19]

Many jurisdictions lack this degree of legal guidance, simply mandating that intermediaries take action against content that comes to their 'knowledge' as being in violation of a law.[20] These laws are often unclear on the meaning of 'knowledge' and whether a simple notice from a private entity suffices as a trigger for action by the intermediary. Consequently, many international internet companies devise their own grievance redress mechanisms to comply with the legal requirement.[21] As will be discussed below, notice and takedown systems may require clear procedural protections in order to avoid removing lawful online speech and information, and in order to comport with requirements of the OAS human rights framework.

By contrast, some countries like Canada have created "notice and notice" mechanisms.[22] This model has also found part of the proposed Copyright Bill in Hong Kong.[23] These mechanisms create an obligation that the intermediaries "convey to the user notices of the alleged unlawfulness of a particular expression," but not an obligation to remove content based on a mere accusation of

---

[17] 17 U.S.C. 512.

[18] *See generally*, Department of Commerce DMCA Multistakeholder Forum, *DMCA Notice-and-Takedown Processes: List of Good, Bad, and Situational Practices*, https://www.uspto.gov/sites/default/files/documents/DMCA_Good_Bad_and_Situational_Practices_Document-FINAL.pdf [https://perma.cc/3KDM-JBSW].

[19] Urban et al, *Notice and Takedown in Everyday Practice* (2016) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628; *See also* Daphne Keller, *Empirical Evidence of "Over-Removal" by Companies Under Intermediary Liability Laws,* (Oct. 12, 2015), http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws [https://perma.cc/93U6-SSXG].

[20] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), 2000 O.J. L 178, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN [https://perma.cc/HR5P-FDZT].

[21] *See, e.g.,* Amazon- https://www.amazon.com/gp/help/reports/infringement [https://perma.cc/WNQ7-LD6H].

[22] Copyright Modernization Act of Canada, World Intermediary Liability Lab: Canada; IACHR, OSRFE, (2013) *infra* note 24 at 109.

[23] Copyright Amendment Bill, World Intermediary Liability Map: Hong Kong: http://cyberlaw.stanford.edu/page/wilmap-hong-kong [https://perma.cc/XY64-YU3M].

unlawfulness or infringement.[24] For "notice and notice" to provide meaningful protection to users and content creators, the OSRFE has said that it must satisfy a few requirements. First, notices to accused users must "include a detailed notice about the location of the material considered unlawful and the legal basis for the unlawfulness. . . ."[25] Second, there must be "an adequate option for counter-notice to the user who produced the content, with judicial oversight guarantees."[26] Finally, users must have the right to retain anonymity and have any dispute regarding such notice "resolved exclusively in court."[27]

Finally, some laws mandate that an intermediary must face no liability or obligation to remove user content unless it has received a court order deeming the content illegal. In some cases, court orders are required as per the statute, for instance in Brazil's Marco Civil[28] and Chile's copyright law.[29] In other cases, variations on this standard have been interpreted into the law by courts, as in India and Argentina.[30]

3. Strict Liability Approach

The most extreme approach to intermediary liability is the strict liability model, holding intermediaries liable for content shared by their users even if the intermediary did not engage with the content or have any knowledge of it. We are unaware of jurisdictions that follow a strict liability approach in legislation. In rare cases, however, courts have accepted a strict liability standard. For example, in *Delfi v. Estonia*,[31] the ECtHR upheld an Estonian court holding that a news portal was liable for hate speech in comments posted by users, even before becoming aware of the comments. As the dissent in that case pointed out, this effectively means that intermediaries must proactively monitor and delete users' posts -- with inevitable chilling effects from intermediaries removing lawful but controversial speech in order to avoid potential legal risk. A subsequent ruling from the same court rejected a strict liability standard for intermediaries hosting merely defamatory speech, because of this threat to users' expression and information rights.[32] The Argentine Supreme Court also rejected strict liability for intermediaries, based on careful review of the threat to online speech

---

[24] IACHR Office of the Special Rapporteur for Freedom of Expression (OSRFE), *Freedom of Expression and the Internet*, (Dec. 31, 2013), at para 109 https://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pdf [https://perma.cc/6GZV-GAYX].

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] Marco Civil da Internet - "Brazilian Internet Bill of Rights," Federal Law no. 12.965, April 23, 2014, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm [https://perma.cc/PCJ3-RJ3H].

[29] Chilean Law 20,430 (modifying Law 17,336 on Intellectual Property), Diario Oficial D.O., May 4, 2010 https://www.cdt.org/files/file/ChileanLaw20430-ModifyingLaw17336.pdf [https://perma.cc/7ZUC-XHS9]. C.f. Chile's Notice and Takedown System for Copyright Protection: An Alternative Approach, (Aug. 2012), https://cdt.org/files/pdfs/Chile-notice-takedown.pdf [https://perma.cc/RQ5C-NG5L].

[30] Corte Suprema de Argentina, "Rodríguez M. Belen c/Google y Otro s/ daños y perjuicios," Judgment R.522.XLIX, 10/28/14 (*Belen Rodriguez)* & Shreya Singhal v. Union of India, (2015) 12 SCC 73.

[31] [2015] ECHR 586

[32] Magyar Tartalomszolgaltatok Egyesulete v. Hungary, [2016] ECHR 135

rights.[33]

C. Intermediary Liability and Users' Free Expression Rights

The scope of permissible intermediary liability laws is shaped by human rights considerations. Legal frameworks that lead intermediaries to remove lawful speech from their platforms may violate a state's human rights obligations. In recent years, human rights bodies have been increasingly outspoken on the topic of intermediary liability and Internet users' rights to seek and impart information.

1. Intermediary Liability and Expression Rights in Human Rights Documents

Intermediaries play an important role in connecting users to the internet and enabling access to information and expression online.[34] The United Nations Human Rights Council ('UN HRC') has called for online rights equal to the rights that people have offline in accordance with the Universal Declaration of Human Rights ('UDHR') and the International Covenant on Civil and Political Rights ('ICCPR').[35] As suggested by their names, intermediaries play an important role in the providing a bridge between users and their rights.

Article 19 in both the ICCPR and UDHR guarantees the freedom of expression to persons.[36] This includes rights to "hold, seek, receive and impart" information across all fora regardless of form. Article 19 of the UDHR mandates the freedom of opinion and expression regardless of media/frontiers.[37]

The American Convention on Human Rights ('ACHR') also guarantees the freedom of thought and expression.[38] As recognized by Article 13 of the ACHR, "everyone has the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice." The ACHR along with Article IV of the American Declaration[39] and Article 4 of the Inter-American Democratic Charter[40] have been read to give more robust protections to unrestricted expression

---

[33] *Belen Rodriguez*, Judgment R.522.XLIX (2014)

[34] Article 19, (2013) *supra* note 4.

[35] Resolution on the promotion, protection and enjoyment of human rights on the Internet (June 2016) United Nations Human Rights Council, *http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20* [https://perma.cc/92H4-PDW7] (UN HRC Resolution on Promotion of HR)

[36] The Universal Declaration of Human Rights, http://www.un.org/en/universal-declaration-human-rights/ [https://perma.cc/GM57-9TX8]; International Covenant on Civil and Political Rights, http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx [https://perma.cc/5R35-9SPP].

[37] The ICCPR General Comment No. 34 provides a deeper analysis of the Article 19 mandate. It has been analyzed specifically under Appendix B of this Report.

[38] American Convention on Human Rights "Pact of San Jose, Costa Rica", B-32, https://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.pdf [https://perma.cc/B843-T2JX].

[39] American Declaration of the Rights and Duties of Man, ("American Declaration") http://www.cidh.oas.org/Basicos/English/Basic2.american%20Declaration.htm [https://perma.cc/8QVV-YY6J].

[40] Inter-American Democratic Charter, http://www.oas.org/charter/docs/resolution1_en_p4.htm

than provided by the UDHR and ICCPR,[41] being referred to as,

> the international framework that provides the greatest scope and the broadest guarantees of protection to the right to freedom of thought and expression.[42]

In light of these uniquely strong protections, the OSRFE has said that:

> restrictions provided for in other international instruments are not applicable in the American context, nor should such instruments be used to interpret the American Convention restrictively.[43]

In addition, the ACHR contains provisions that are particularly relevant for the issue of intermediary liability for online expression and access. Article 13.3 provides:

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

This express prohibition on indirect censorship through control of "equipment used in the dissemination of information" is highly relevant for laws that oblige internet intermediaries to restrict the flow of online information. The OSRFE spoke strongly to this issue in its 2016 Report, stating that "[t]he [intermediary] liability regime is fundamental for creating the appropriate incentives for the protection and guarantee of human rights."[44] Further, the need for any restriction so imposed to be in accordance with the primacy of the right of speech protected by Article 13 of the ACHR has been emphasized by the OSRFE.[45]

Despite this broad protection for online speech and information, there remain narrow instances in which governments may permissibly oblige intermediaries to suppress online content. Discussing Article 19, the UN's Office of the High Commissioner for Human Rights commented that "the exercise of the right to freedom of expression carries with it special duties and responsibilities and . . . certain restrictions . . . are permitted . . . ."[46]

Under the international human rights law and within the Inter-American system, permissible restrictions -- as well as key substantive and procedural limits on such restrictions -- must comply with the three-step test. The three-step test provides the framework for evaluating

---

[https://perma.cc/QE47-TA9J].

[41] IACHR, OSRFE, (2010) *supra* note 3 at 2; IACHR, OSRFE, (2013) *supra* note 24 at para 1.

[42] IACHR, OSRFE, (2010) *supra* note 3 at 14.

[43] IACHR, OSRFE, (2010) *supra* note 3 at 2.

[44] IACHR OSRFE, *Standards for a Free, Open & Inclusive Internet* (2017) 44, para 104, https://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf [https://perma.cc/SC2U-FDYR].

[45] IACHR, OSRFE, (2013) *supra* note 24 at para 14.

[46] Comment no. 10 on Article 19 of Universal Declaration of Human Rights 1948, Article 19.

the legality, legitimacy and proportionality of such restrictions.[47]

Pursuant to Article 13 of the ACHR and its interpretative bodies, the following three conditions must be met in order for a restriction on free expression to be permissible:

(1) The limitation must have been defined in a precise and clear manner by a law, in the formal and material sense,[48]

(2) the limitation must serve compelling objectives authorized by the Convention;[49] and

(3) the limitation must be necessary in a democratic society to serve the compelling objectives pursued, strictly proportionate to the objective pursued, and appropriate to serve said compelling objective.[50]

Importantly, restrictions may not be used as a method of prior censorship,[51] applied in a manner that is discriminatory,[52] or used as an indirect method for abuse/impeding expression.[53] The three-step test may be explained as follows:

Step 1: "The limitation must have been defined in a precise and clear manner by a law, in the formal and material sense"

In order to be legitimate, a restriction on freedom of expression must be clearly established in the text of a law. The Legal Framework states that the law must unambiguously specify the grounds for which liability may be imposed for the exercise of free expression.[54] Vague, ambiguous, broad, or open-ended laws give authorities "very broad discretionary powers,"[55] and may lead to arbitrariness and prior censorship. This may "discourage the dissemination of information and opinions out of fear of punishment, and can lead to broad judicial interpretations that unduly restrict freedom of expression."[56]

The Legal Framework is designed to "be more generous and to reduce to a minimum the

---

[47] IACHR OSRFE (2013) *supra* note 24 at 55. Frank La Rue notes that any restriction applied to freedom of expression online must comply with international human rights laws, including the three-step test as will be discussed. Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN HRC, A/66/290, http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf [https://perma.cc/V25Z-PF9H].

[48] IACHR, OSRFE (2010) *supra* note 3 at 69-73.

[49] *Id*. at 74-82.

[50] *Id.* at para 84-89;

[51] *Id*. at 91-92.

[52] *Id*. at 93-95.

[53] *Id*. at 96-97.

[54] *Id.* at para 69.

[55] IACHR, OSRFE, *Freedom of Expression Standards for Free & Inclusive Broadcasting*, (2010) at para. 131. IACHR, OSRFE (2010) *supra* note 3 at para 70.

[56] IACHR, OSRFE (2010) *supra* note 3 at para 71.

restrictions to the free circulation of information, opinions, and ideas"[57] in comparison to the provisions of international human rights treaties—including, the European Convention for the Protection of Human Rights and Fundamental Freedoms.

As will be explained in Part IV, the European Court of Human Rights (ECtHR) have developed the idea of the "defined in a precise and clear manner by a law" standard in the intermediary liability context in *Ahmet Yildirim v. Turkey* case (*Yildirim*).[58]

Step 2: "Designed to achieve one of the compelling objectives authorized by the Convention"

Article 13 of the ACHR lists two compelling objectives justifying restrictions on free expression: (1) "respect for the rights or reputations of others" or (2) "the protection of national security, public order, or public health or morals."

Regarding the first objective, the IACHR and the Inter-American Court of Human Rights ('IACtHR') emphasize "balancing and harmonization whenever the exercise of freedom of expression conflicts with the right of others to their honor, reputation and good name,"[59] but note that the right to free expression has greater weight than the honor of a public official, as "expressions regarding the practices of State institutions enjoy greater protection."[60] This standard will be explored further in Part IV, discussing RTBF laws under the OAS system.

With respect to the second objective, it is important to note that "any impairment of public order that is invoked as a justification to limit freedom of expression must be based on real and objectively verifiable causes that present the certain and credible threat of a potentially serious disturbance of the basic conditions for the functioning of democratic institutions."[61]

The 2011 Joint Declaration on Freedom of Expression and the Internet[62] ('2011 Joint Declaration'), to which the OSRFE is a signatory, likewise specifies that "compelling objectives" be narrowly tailored.

---

[57] IACHR, OSRFE (2010) *supra* note 3 at 2.

[58] Application No. 3111/10, (Dec. 18, 2012), ECtHR, http://hudoc.echr.coe.int/fre?i=001-115705 [https://perma.cc/B5WQ-BBKT].

[59] IACHR, OSRFE (2010) *supra* note 3 at para 76.

[60] *Id.* at 105.

[61] *Id.* at 82. (The court defines "public order" as "the conditions that assure the normal and harmonious functioning of institutions based on a coherent system of values and principles." It notes that public order depends on a functioning democracy, which in turn relies on the protection of free expression to ensure "widest possible circulation of news, ideas, and opinions as well as the widest access to information by society.")

[62] Joint Declaration on Freedom of Expression and the Internet, (June 1, 2011) http://www.osce.org/fom/78309 [https://perma.cc/V34X-HHFT].

Step 3: "Necessary in a democratic society to serve the compelling objectives pursued, strictly proportionate to the objective pursued, and appropriate to serve such compelling objective."

As articulated by the UN HRC, this criterion requires states to show that a restrictive measure is appropriate by "demonstrat[ing] in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat."[63]

i) interpretations of "necessity"

In the OSRFE's formulation, a measure may be deemed "necessary" if there is a "clear and compelling need for its imposition" and it "cannot reasonably be accomplished by any other means less restrictive to human rights."[64] Thus, the state has the burden of proving that there is a "clear harm or threat of harm to the rights of others," and there are "clear and precise legal provisions establishing such subsequent liabilities for the conduct causing these harms."[65] A measure fails the "test of necessity if the protection could be achieved in other ways that do not restrict freedom of expression."[66]

ii) interpretations of "proportionality"

The IACtHR sets forth three factors that establish the proportionality of a restriction on freedom of expression imposed for the purpose of preserving other rights: "(i) the degree to which the competing right is affected (serious, intermediate, moderate); (ii) the importance of satisfying the competing right; and (iii) whether the satisfaction of the competing right justifies the restriction to freedom of expression."[67]

In the Intermediary Liability context, human rights organizations have interpreted the "necessity" and "proportionality" requirements as grounds for procedural protections in notice and takedown systems. As will be discussed in more detail below, the Manila Principles require that "laws, orders, and practices restricting content must be necessary and proportionate in a democratic society," meaning specifically that they must be "limited to specific content at issue," use the "least restrictive technical means," and be appropriately limited in geographic scope and duration.

The "least restrictive means" by which a government can respond to or restrict illegal content is defined as "the least intrusive instrument amongst those which might achieve the desired result."[68] In other words, government actors or ISPs employ the "least restrictive means" when

---

[63] General Comment No. 34 on Article 19 of the ICCPR (2011), http://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf [https://perma.cc/22EM-EPT5].

[64] IACHR, OSRFE (2010) *supra* note 3 at para 85.; *Id.* (A measure fails the "test of necessity if the protection could be achieved in other ways that do not restrict freedom of expression.")

[65] *Id.* at para 107.

[66] General Comment No. 34 on Article 19 (2011) *supra* note 62.

[67] *Id.* at para 89.

[68] General Comment 27 at para 14.

they block the least amount of content possible that would still enable them to fulfill their legal objectives.

iii) interpretations of "appropriate"

To be deemed appropriate, a measure must be "effectively conducive to attaining the legitimate and compelling objectives in question."[69] Restrictive measures "must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected."[70] This test for appropriateness was addressed by the ECtHR in the *Yildirim*.[71]

The ECtHR held that the judicial restriction should be "based on a weighing-up of the competing interests at stake and designed to strike a balance between them."[72] During the discussion, the court mentioned that the interest of the law underlying the entire blocking order should be considered together with the rule of proportionality, the rights of internet users, and other significant collateral effect against the democratic society.

The three-step test of Article 13 has been applied specifically in the context of SSB in Part IV of this Report.

2. Procedural Protections and The Manila Principles on Intermediary Liability

A key document in the literature of intermediary liability and human rights is the Manila Principles on Intermediary Liability.[73] Drafted and endorsed by civil society groups from around the world, the Manila Principles set forth concrete practices and proposed legal standards to safeguard human rights when intermediaries are asked to restrict online content. The proposals are in many cases backed up by human rights literature from the OSRFE and other sources. Correspondingly, the OSRFE has also used the Manila Principles as a "reference framework of baseline safeguards and best practices for States with regard to intermediary liability based on international human rights instruments" in the past.[74] These principles include:

1. Manila Principle 2 - Independent and Impartial Adjudication of Restrictions

Manila Principle 2 states that "[i]ntermediaries must not be required to restrict content unless an order has been issued by an independent and impartial judicial authority that has determined that the material at issue is unlawful."[75] This strong requirement for judicial

---

[69] *Id* at para 87.

[70] Human Rights Committee, General Comment 27, Freedom of movement (Art.12), U.N. Doc CCPR/C/21/Rev.1/Add.9 (1999), para 14, http://hrlibrary.umn.edu/gencomm/hrcom27.htm [https://perma.cc/V2LX-EQY7].

[71] *Yildirim* No.3111/10, (2012), ECtHR at para.

[72] *Id.* at para 64.

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

[74] IACHR, OSRFE, (2017) *supra* note 44 at 46.

[75] Manila Principle 1 calls for clear intermediary liability shields in law. We do not elaborate on it here because it

adjudication finds support in the 2017 Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda[76] ('Joint Declaration on Fake News'), in which the OSRFE and other rapporteurs state that:

> Intermediaries should never be liable for any third-party content relating to those services unless they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it and they have the technical capacity to do that.

The OSRFE in 2013 stated a similar standard under the "conduit principle," restricting liability for intermediaries unless they "specifically intervene in that content or refuse to obey a court order to remove" it,[77] but acknowledging that in "extraordinarily exceptional" cases, requiring intermediaries to remove content based on notice from a private party may not create a risk of private censorship.[78]

The Argentine Supreme Court adopted a modified version of this standard in the *Belen Rodriguez* case.[79] In *dicta*, it stated that in cases of unclear legal claims, intermediaries should only remove content based on judicial determination. An intermediary

> cannot be required to carry out the tasks of the competent authority, let alone that of judges. For these reasons, in these cases it is necessary to require a competent judicial or administrative notice, as the simple communication of the aggrieved individual or any other interested party is not sufficient.[80]

By contrast, the court said, where the unlawful nature of content and the damage is evident and clear, notice from a private party may create "actual knowledge" and liability for the intermediary if it does not remove the content.[81]

2. Manila Principle 4 - Orders Must Be Necessary and Proportional

The fourth Manila Principle states that laws restricting online content "must be necessary and proportionate in a democratic society," adopting "the least restrictive technical means" of

---

does not provide additional specific notice and takedown procedural protections.

[76] Joint Declaration On Freedom Of Expression And "Fake News," Disinformation And Propaganda (2017), https://www.coe.int/en/web/media-freedom/-/joint-declaration-on-freedom-of-expression-and-fake-news-disinformation-and-propaganda [https://perma.cc/JZC9-WRUL].

[77] IACHR OSRFE (2013) *supra* note 24 at 41.

[78] *Id.* at para 105. *See also* Guide to Human Rights for Internet Users, Recommendation CM/Rec (2014)6 and explanatory memorandum, at 16. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31 [https://perma.cc/QP9P-NYER] ; UN HRC, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27 at 20; OSCE, *Freedom of Expression on the Internet*, (2012), 52 http://www.osce.org/fom/105522?download=true [https://perma.cc/C8R3-VSHC].

[79] *Belen Rodriguez*, Judgment R.522.XLIX (2014).

[80] *Id.* at para 18.

[81] *Id.*

restriction. In this respect, it mirrors Part 3 of the ACHR, Article 13, as well as standards derived from Article 19 of the UDHR and the ICCPR.[82] As spelled out in Manila Principle 4, this includes limits on the temporal duration of a restriction and, when consistent with the intermediary's services, limits on geographic scope. Consistent with this principle, content that is blocked for being unlawful in a particular jurisdiction must only be blocked in that jurisdiction.

In the Joint Declaration on Fake News, representatives of the UNHR, OSCE, OAS and ACHPR together addressed the jurisdictional scope of content restrictions. They noted that, in the narrow cases in which states may legitimately restrict speech under the three-step test, free expression standards nonetheless

> apply regardless of frontiers so as to limit restrictions not only within a jurisdiction but also those which affect media outlets and other communications systems operating from outside of the jurisdiction of a State as well as those reaching populations in States other than the State of origin.[83]

Geographic and temporal scope limitations identified Manila Principle 4 can be extremely important for maintaining the necessity and proportionality of a restriction. For instance, as discussed in the RTBF section of this Report, the scope of right to privacy and data protection in all countries is different. As a result, the *Google Spain* decision,[84] which follows European law, may not have the same implementation in the OAS countries. Therefore, any restriction imposed under the decision is best curtailed geographically only to the applicable countries and not across the globe. Similarly, as discussed in the site blocking section of this Report, orders compelling intermediaries to block entire websites -- rather than blocking individual unlawful pages -- may fail to meet the "least restrictive means" requirement.

3. Manila Principles 3 and 5 - Respect for Due Process

The Manila Principles No. 3 and 5 address different procedural requirements to protect the rights of internet intermediaries and users. Principle 3 primarily focuses on the court order or notice to an intermediary that triggers removal, while Principle 5 deals mostly with appeal and redress once a removal has taken place. These two Principles track the OSRFE's 2013 statement that "orders or notices need to state precisely which content must be removed, thus keeping legitimate expression from being affected," and that states should establish "necessary safeguards," including "access to an effective remedy, so as to limit the risk of abuse in the adoption of these types of measures."[85] As the OSRFE further explained, these systems "need to have certain requirements

---

[82] UNESCO, Keystones to foster inclusive Knowledge Societies: *Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet*, at 38, http://unesdoc.unesco.org/images/0023/002325/232563E.pdf [https://perma.cc/6ZFL-HBJ9] ("[T]he international standard requires that any restrictions need to be enacted by law, should only be imposed for legitimate grounds as set out in the UDHR and ICCPR, and must also conform to tests of legality, necessity and proportionality.")

[83] Joint Declaration on Fake News, at para. 1.c.

[84] *See* discussion *infra* Part III.

[85] IACHR OSRFE (2013) *supra* note 24 at para 107.

to be legitimate from the point of view of protection of freedom of expression."[86]

Manila Principle 3 elaborates on the requirements for valid orders or notices, listing information that any such communication to an intermediary must provide. It also requires penalties for those who act in bad faith to achieve removal of lawful content, and furthers the idea of introducing a "notice and notice" system where possible. To provide the intermediary with adequate notice, the court order must include the Internet identifier and description of the unlawful content, evidence sufficient to document the legal basis of the order, and the time period for which the content should be restricted.[87] Concrete examples of notice requirements in national law include the U.S. DMCA[88] and the standards discussed in the EU *Telekabel* case.[89]

Manila Principle 5 requires an effective right to be heard for both intermediaries and the users whose rights are affected by content restrictions, and specifies both a right of appeal and right to reinstatement of wrongly removed content. In addition to tracking the OSRFE's call for effective remedies, Principle 5 aligns with the 2016 Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression ('UN Special Rapporteur'), which urges improved remedial or grievance mechanisms for Internet users affected by removal of their online expression—meaning that users must receive adequate notice of the restriction and an opportunity to contest it.[90]

European organizations have expressed similar views on transparency and due process. The Committee of Ministers of the Council of Europe, for example, notes that states have the responsibility to embrace "the right of independent appeal, surrounded by appropriate legal and due process safeguard."[91] One aspect of this right was mandated by the European Court of Justice ('CJEU') decision in *Telekabel*. That ruling affirmed national courts' ability under EU law to order ISPs to block websites, using orders that do not specify the technical means of blocking, but required as a safeguard mechanism for internet users that "the 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."[92]

---

[86] *Id.* at para 97.

[87] The Manila Principles on Intermediary Liability Background Paper at 27, https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf [https://perma.cc/BS9P-ETMN].

[88] 17 U.S.C. 512.

[89] C-314/12, Telekabel Wien GmbH v Constantin Film Verleih GmbH, ECLI:EU:C:2014:192.

[90] A/HRC/32/38 (2016).

[91] Recommendations and Declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, Media and Internet Division, Directorate General of Human Rights and Rule of Law, Strasbourg, (July 2015) at 334, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44 [https://perma.cc/277F-Q5SA].

[92] *Telekabel*, 2014 E.C.R. I-00000, ¶ 57; *see also* Martin Husovec, *CJEU Allowed Website Blocking Injunctions with Some Exceptions*, (March 27, 2014), http://www.husovec.eu/2014/03/cjeu-allowed-website-blocking.html [https://perma.cc/E88Z-H5C5].

4. Manila Principle 6 - Transparency

The Manila Principles also echo human rights sources in emphasizing the need for transparency and accountability, requiring both the government and the intermediaries to clearly share information on laws, policies and specific decisions concerning access to online content.[93] When possible, Principle 6 requires intermediaries to display "a clear notice" to Internet users who attempt to access blocked or removed content, specifying "what content has been restricted and the reason for doing so."

Catalina Botero Marino strongly endorsed transparency in her 2013 report, saying that

> [w]ith respect to the duty of transparency, intermediaries should have sufficient protection to disclose the requests received from government agencies or other legally authorized actors who infringe upon users' rights to freedom of expression or privacy. It is good practice, in this respect, for companies to regularly publish transparency reports in which they disclose at least the number and type of the requests that could lead to the restrictions to users' rights to freedom of expression or privacy.[94]

The report further suggests that national laws should enable transparency reporting.[95] The UN HRC 2011 report similarly called upon member States to "provide lists of blocked websites and full details regarding the necessity and justification for blocking each individual website. An explanation should also be provided on the affected websites as to why they have been blocked."[96] Without such notice, individuals in the OAS would be effectively unable to exercise their rights, under Article 25, to recourse when their rights have been affected. Recently, the OSRFE has deemed the transparency measures about content removed or blocked as "essential in order to properly control the legality of these measures."[97] While our research found no case law regarding notice to users seeking blocked online content in the Inter-American jurisprudence, a UK court decision has adjudged such a notice to be an important safeguard when ISPs are ordered to block online content.[98] Notice of blocked or removed content would also seem necessary for Internet users to exercise the right of appeal laid out in the CJEU *Telekabel* case, discussed above.

Widespread calls for increased legal requirements and frameworks of transparency have had relatively modest effect to date. While a few companies like Google release transparency reports with empirical data on requests received and notify users when the content they posted or content they seek has been removed,[99] this transparency is often patchy. The release of some of this data is restricted in several jurisdictions.[100] In some cases, as with the RTBF in the EU, the

---

[93] Principles 6.a-d and g, Manila Principles.

[94] IACHR OSRFE (2013) *supra* note 24 at 51.

[95] *Id.* at 113. *See also* A/HRC/17/27 at 21.

[96] A/HRC/17/27 at 20.

[97] IACHR, OSRFE, (2017) supra note 44 at 50.

[98] Cartier International AG v. BSB, [2014] EWHC 3354 (Ch) (safeguards established by courts against abuse have been discussed *infra* Appendix A).

[99] OECD, (2011) at 34. Several other intermediaries release transparency reports including Yahoo, Microsoft, Twitter, Facebook, Automattic.

[100] A/HRC/32/38, (2016) at 22 (Transparency is important across the board, including in the context of content

law may affirmatively bar intermediaries from informing users when particular links or content have been removed.[101] Where intermediaries do provide transparency, such action is typically volitional by the companies and not required by law; and transparency reporting from governments and private notifiers -- as opposed to intermediaries -- is rare. An important organization in this regard is the Global Network Initiative, which urges transparency by member companies.[102]

Transparency reporting and the data collected thereunder can provide some useful insights on how to create due process safeguards to avoid overreaching or illegal blocking of content.[103] Intermediaries that prioritize transparency and open communication regarding implemented blocks are in a position to enable individuals to understand the limits placed on their freedom of expression online and seek appropriate redress when their rights are violated.[104]

D. Issues analyzed in this Report

Part IV of the Report delves deeper in the RTBF doctrine. It explores the inherent conflict between the RTBF and freedom of expression. Analyzing the decision from the European Union, it identifies four distinct elements of the ruling and discusses whether each can be reconciled with OAS human rights framework. Human rights consideration affect both substantive balancing of privacy and expression rights and procedural questions about relying on search engines to decide which webpages must be de-listed. It concludes that many aspects of the RTBF as defined by EU courts may not be reconcilable with the OAS system.

Similarly, Part V of the Report delves into blocks that affect entire websites, services and mobile applications. It explores the application of the three-step test to government and court orders that implement these blocks, and highlights precautionary measures from international human rights documents. It identifies relevant transparency, accountability and due process considerations to protect freedom of expression.

The RTBF and the SSB portions of the report also identify trends based on our review of some -- though not all -- recent developments within OAS states. The RTBF trends include judicial reliance on data protection legal frameworks, which may displace conventional analysis of free expression threats under the three-step test or OAS intermediary liability rules. The SSB trends include the lack of clear legal basis and procedural safeguards to protect freedom of expression rights, and the disproportionate use of SSB orders by courts in some countries.

---

regulation, and should include the reporting of government requests for takedowns.); UNESCO highlights several laws in South Africa, UK and India that prohibit such disclosures, A/HRC/32/38 at 17-18.

[101] *See* discussion *infra* Part III.

[102] Global Network Initiative is a multi-stakeholder group of industry players, civil society organisations, investors and academics, http://globalnetworkinitiative.org [https://perma.cc/Q6GT-79PN].

[103] *See generally*, Article 19 (2013) *supra* note 4 at 2.

[104] A/HRC/32/38, (2016) at 17 ("Transparency can help ensure that subjects of Internet regulation are able to meaningfully predict their legal obligations and challenge them where appropriate. Gaps in compliance with these standards threaten the ability of individuals to understand the limits placed on their freedom of expression online and seek appropriate redress when their rights are violated.").

Each part of the Report analyzes the substantial and procedural human rights affected by these emerging trends, and considers possible solutions from human rights instruments and documents interpreting them. Each concludes by discussing options and next steps the OSRFE could take to guide OAS states in assessing RTBF and SSB claims in light of free expression and other human rights.

PART III: RIGHT TO BE FORGOTTEN

A. Introduction

This Part of the Report uses the ACHR framework to analyze the concept of the Right To Be Forgotten (RTBF) and its main components as developed by the CJEU and interpreted by adjudicatory bodies around the world. By reviewing selected cases, decisions, and human rights sources from OAS countries as well as countries outside of the OAS region that have aligned or markedly departed from the OAS countries' approach, our purpose is to identify emerging policy trends and assess how they might be treated under the OAS human rights framework.

The Internet has presented many challenges to laws regulating expression and information since the early 1990s. More recently, and as the Internet has become increasingly pervasive in how information is conveyed, the freedoms to express and receive information appear in particular tension with the right to privacy and personal data protection. Although specific national laws differ, some countries see a conflict between these two sets of rights when applied to search engines that index content generated by third parties. Some see the role of search engines in a positive light, as facilitators of instantaneous access to previously remote information, and as an incredible means to make the world's information available. But others see a threat, worrying that content made more accessible by search engines may endanger individual rights like privacy and reputation.

This debate is particularly interesting in the context of the OAS human rights system, given its unique provisions and guidance on both freedom of expression and intermediary liability. Although the most famous case on the RTBF — *Google Spain v. Agencia Española de Protección de Datos & Mario Costeja González* ("*Google Spain*")[105] — was decided by the CJEU in 2014, RTBF claims based on data protection rights have received attention in several OAS countries, including Colombia, Mexico and Peru. The European approach is highly relevant because many OAS countries have data protection regimes modeled on the law applied in the *Google Spain* case: the 1995 EU Data Protection Directive ('Data Protection Directive').[106] At the same time, given the different legal traditions and approaches to human rights concepts in the two regions, there may be no universal interpretation of data protection laws or of the RTBF. Our research draws out key elements of the European RTBF in order to evaluate its compatibility with the ACHR. It further examines RTBF-related trends within the OAS and other regions, and their relation to free expression and other human rights obligations.

This chapter is divided into six sections. The following section outlines the RTBF and its

[105] European Court of Justice, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, May 13, 2014.

[106] Keller, *Europe's Right to be Forgotten in Latin America,* Towards an Internet Free of Censorship II Perspectives in Latin America, at 2-3, http://www.palermo.edu/cele/pdf/investigaciones/Towards_an_Internet_Free_of_Censorship_II_10-03_FINAL.pdf [https://perma.cc/B2ER-FET2] (English) and http://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf [https://perma.cc/MM96-Q5KU] (Spanish); *See also* Directive 95/46/EC.

main elements as developed by the CJEU in *Google Spain*. The next section, Section C, tries to understand the European RTBF concept under the ACHR and its interpretative sources. Section D analyzes trends arising from the application of the RTBF in OAS countries, as well as other countries around the world. The following section draws out a series of next steps that the client could take to get a more comprehensive perspective around the implementation of the RTBF concept in the region. We provide our conclusions in Section F. Brief snapshots of the key issues in the cases analyzed in section D are set out in the Appendix A to this Report.

B. The Right To Be Forgotten Concept

The RTBF rose to prominence globally in 2014. While defined differently by various speakers, as conceived in the EU it is a right based on data protection laws for individuals to compel search engines to de-list certain search results pertaining to them. This framing arose from the controversial *Google Spain* judgment of the CJEU, which ignited a zealous debate about the proper balance between freedom of speech and the protection of personal data. Neither the *Google Spain* analysis nor the underlying Data Protection Directive refer explicitly to a RTBF. However, the right established in the case was soon given this name in popular, academic, and policy discussions.

The RTBF emerging from the *Google Spain* judgment is focused predominantly on search engines. Accordingly, the RTBF represents a remedy pursuant to which an individual may request that the operator of a search engine remove links to third parties' web pages containing his/her personal data, when those links appear in results for search queries based on the individual's name.[107] The RTBF is not absolute, and the CJEU clarified that it must be balanced against the public interest and against competing fundamental rights.[108] Where that balance favors de-listing search results, the *Google Spain* judgment does not require the content to be erased from particular web pages, nor does it require search engines to de-list results for all queries. Instead, it requires the search engine to de-list the web page only from the search results based on the individual's name.

The RTBF is an evolving concept. The RTBF, where it is supported by law at all, is interpreted and applied differently around the world, partially for historical reasons. One major source of difference may be that the EU recognizes the protection of personal data as a fundamental human right, but other regions or countries may not. For example, the United States does not have such a right in the U.S. Constitution. Legal cultures also differ in providing a possibility for the individual to "start anew." In some countries, the concept of the RTBF goes back to the 1960's with the recognition of the *droit à l'oubli.*[109] Others saw similar laws prior to the *Google Spain*

[107] *Google Spain* at para 3 from Ruling.

[108] Google Spain C-131/12 (2014) at para 97. Historically, the European courts have aimed to balance the right to privacy and the right to freedom of expression. The Charter of Fundamental Rights of the European Union contains the fundamental rights recognised by the European Union, including the right for private and family life, the right of protection of personal data and the right of freedom of expression and information. The *Google Spain* judgment refers to the aforementioned document on several occasions.

[109] The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten', Alessandro Mantelero; published by Computer Law & Security Review, Volume 29, Issue 3, June 2013 (http://www.sciencedirect.com/science/article/pii/S0267364913000654 [https://perma.cc/49Y7-8GWW]).

allowing individuals to suppress true information, such as spent criminal convictions.[110] Even after the CJEU's ruling, some cases have expanded the scope of the narrowly defined right in the *Google Spain* judgment and applied it beyond search engines to the source of the information (e.g. news archives).[111]

1. Elements of the EU RTBF Under the *Google Spain* Judgment

The name of Mario Costeja González, a Spanish citizen, initially appeared in La Vanguardia's newspaper upon order by Spain's Ministry of Labour and Social Affairs in relation to "a real-estate auction with attachment proceedings for the recovery of social security debts."[112] Over ten years later, Mr. Costeja González found Google search results pointing to a digitized version of the page, and lodged a complaint with the Spanish Data Protection Authority ("AEPD") against La Vanguardia Ediciones SL, Google Spain SL and Google Inc. Mr. Costeja Gonzales wanted La Vanguardia to remove the pages referring to him, and for Google to remove personal data relating to him from its search results, so that the links related to his outdated debts that identified him would no longer be public.[113] The AEPD rejected the complaint concerning La Vanguardia but it upheld the complaint against Google. Spanish courts reviewed the case and referred it to the CJEU.

In its ruling, the CJEU upheld Mr. Costeja Gonzalez's claim and held that data protection law compelled Google to de-list certain search results upon request. The elements established by the CJEU with respect to the *Google Spain* case along with relevant regulatory interpretations are explained in the following paragraphs.

a) The definition of the RTBF: De-listing obligation of a search engine as a "controller" subject to data protection law

As a matter of data protection law, the CJEU's ruling rested on three key grounds. First, the CJEU held that Google was "established" because it had a subsidiary in Spain that sells advertising space offered by the search engine, which "orientates its activity towards the inhabitants of Spain." Consequently, Google had to comply with the Spanish Data Protection

[110] For example, the decision of a Hamburg court from 2008 pursuant to which the names of two half-brothers convicted of murder had be removed from a popular web page, followed by the reverse decision of the German Constitutional Court taking the side of the freedom of the press [http://freespeechdebate.com/en/case/does-a-murderer-have-the-right-to-be-forgotten/ [https://perma.cc/3DTQ-85JJ]; see also Lawrence Siry, Sandra Schmitz, "A right to Be Forgotten? – How Recent Developments in Germany May Affect the Internet Publishers in the US," European Journal of Law and Technology, Vol.3, No.1, 2012 (https://pdfs.semanticscholar.org/ec95/a0a344f1fc0f7bff948549c76737aae042f8.pdf [https://perma.cc/GZ5F-4KMD]); see also Jennifer Granick, "Convicted Murderer to Wikipedia: Shhh!," Electronic Frontier Foundation (https://www.eff.org/deeplinks/2009/11/murderer-wikipedia-shhh [https://perma.cc/GZ5F-4KMD]).

[111] How Italian courts used the right to be forgotten to put an expiry date on news https://www.theguardian.com/media/2016/sep/20/how-italian-courts-used-the-right-to-be-forgotten-to-put-an-expiry-date-on-news [https://perma.cc/259Z-3Z89].

[112] *Google Spain*, at para 98

[113] *Id.* at para 20

Law.[114] Second, Google's activities represented "processing of personal data"[115] within the meaning of the Data Protection Directive — the operator of the search engine "collects", "retrieves", "records", "organizes" and "makes available"[116] to its users' personal data originally published on indexed web pages, which Google arranges in the form of lists of search results. Third, and critically for the outcome of the case, Google is deemed a "data controller"[117] of indexed website content within the meaning of the Data Protection Directive, because it is the operator of the search engine and determines the purpose and means of processing personal data in the context of its own indexing and other business activities.[118] Based on these key determinations, the court required Google to honor objections or erasure requests by "de-listing" certain results when users searched for the data subject by name.

The ruling went against the Opinion of the CJEU's own influential Advocate General, Nilo Jääskine, issued on June 25, 2013 ('Opinion'). As per the Opinion, the operator of the search engine is not a data controller, because it does not have control over the third parties' web pages, and it does not distinguish between personal and other type of data.[119] It further states that the Data Protection Directive does not create a RTBF that can be invoked against the operator of a search engine.[120] The CJEU disregarded the Opinion and emphasized that the activity undertaken by Google constituted a processing of personal data within the meaning of the Data Protection Directive, and that the reasons for such processing essentially served Google.

b) The standard of the RTBF: "inadequate, irrelevant or no longer relevant or excessive"

The CJEU concluded that individuals have a right to seek de-listing of information that is "inadequate, irrelevant or no longer relevant or excessive."[121] However, de-listing may in some cases be improper based on "the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest

---

[114] *Id.* at para 60.

[115] Pursuant to Article 2 (b) of the Data Protection Directive: "'processing of personal data' ('processing') shall mean 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."

[116] *Google Spain* at para 28.

[117] Pursuant to Article 2 (d) of the Data Protection Directive: "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law[.]"

[118] *Google Spain* at para. 1 of Ruling.

[119] 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), at para 2 of Conclusion, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN [https://perma.cc/8NQ3-JHVA].

[120] *Id.* at para 3 of Conclusion.

[121] *Google Spain* at para. 92, 94.

which may vary, in particular, according to the role played by the data subject in public life."[122] The CJEU did not identify the publisher's free expression interest as a relevant factor. Its conclusion was based on the general principles of data quality envisaged by the Data Protection Directive. It clarified that de-listing may be required even (1) when the information causes no prejudice to the individual,[123] (2) when the information is true,[124] and (3) when the web pages are published lawfully.[125] The CJEU concluded that considering that the web publisher may have different legitimate interests for processing, a webpage may be de-listed even if the webpage itself lawfully processes the data.[126] Finally, the CJEU concluded that data protection rights "override, as a rule" other interests, including Internet users' interests in accessing information.[127]

The CJEU's RTBF analysis aims to ensure that individuals retain control over what data is associated with their name by search engine results. It expresses concern that searches on the basis of the individual's name may have a significant impact on their private life because it provides a "structured overview of the information relating to that individual."[128]

c) The decision-maker of the RTBF: search engines in the first instance

The *Google Spain* ruling requires Google, as a data controller, to assess de-listing requests and comply with them when appropriate. Failure to honor a valid RTBF request would be a breach of the company's duties under the Data Protection Directive and expose the company to fines. The EU's pending General Data Protection Regulation ('GDPR') substantially increases these potential fines -- they can be as high as €20 million or 4% of annual global turnover.[129] Where Google refuses to de-list a result, the data subject may seek review by a Data Protection Agency ('DPA') or a court. Publishers affected by de-listing are not entitled to DPA review.

d) The procedure of the RTBF: Little or no role for publisher

Neither the Google Spain ruling nor the underlying Data Protection Directive provide guidance on key notice-and-takedown procedural issues of the sort addressed in the introduction and in the Manila Principles and other human rights sources. In the wake of the decision, however, the Article 29 Data Protection Working Party, a key EU regulatory organization, elaborated on some points that were not clearly addressed in the CJEU decision. In influential but non-binding guidance, it stated that:

- The data subject is not required to first contact the original source (the webmaster or

[122] *Id.* at para 81.
[123] *Id.* at para 96.
[124] *Id* at para 92.
[125] *Id.* at para 94.
[126] *Google Spain* at para 88.
[127] *Id.* at para 97.
[128] *Id.* at para 80.
[129] GDPR Key Changes, http://www.eugdpr.org/the-regulation.html [https://perma.cc/RXJ5-BUVQ].

publisher) in order to exercise their rights towards the search engine.[130]

- The data subject can contact Google by any means, not only through Google's designated webform.[131]
- Data subjects must "sufficiently explain the reasons why they request de-listing, identify the specific URLs and indicate whether they fulfil a role in public life, or not." They may in some cases also have to provide proof of identity.[132]
- The timeframe and communications in response to a RTBF request are to be governed by national data protection law in each Member State of the EU.[133]
- Google is not permitted to let the webmaster or publisher know when one of its pages has been de-listed based on a RTBF request, because this could identify the data subject and constitute additional impermissible data processing -- though in unusual cases it may consult with a publisher before de-listing.[134]
- Google is not permitted to inform users when particular links or responses to particular search terms are missing based on RTBF claims, because this could effectively identify the data subject.[135]
- If Google rejects a RTBF request, "it should provide sufficient explanation to the data subject about the reasons for the refusal" and inform them of their right to seek recourse from a DPA or court.[136]
- De-listing must be exercised not only on versions of web search targeted to European countries, but on all relevant domains (such as google.es or .com or .mx).[137]

As will be discussed below, the mandate for global removal and the prohibition on routine webmaster notice have both been reinforced by national DPAs in the wake of *Google Spain*. In ongoing litigation in France, the national data protection agency has asserted that de-listings based on French law must be carried out globally, affecting access to information and expression rights for Internet users everywhere in the world.

2. The RTBF Post-*Google Spain*

Following the *Google Spain* judgment, Google received hundreds of thousands of requests for de-listing of search results. To date, Google has evaluated approximately 1,932,339 URLs and

---

[130] Article 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc. v. Agencia Espanola De Proteccion De Datos (AEPD) and Mario Costeja Gonzalez"* C-131/12, (Nov. 26, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf [https://perma.cc/GXN7-TTXY] at Para. 5 of Intro.

[131] *Id.* at 7.

[132] *Id.*

[133] *Id.*

[134] *Id.* at para. 9 of Intro.

[135] *Id.* at para 8 of Intro.

[136] *Id* at 7.

[137] Article 29 Data Protection Working Party, *supra* note 127 at 3, para 7.

received approximately 699,560 requests.[138] Google and Microsoft report that over half of the requests received for their search engines are invalid as per their assessment.[139]

The Article 29 Data Protection Working Party[140] published guidelines on the implementation of the *Google Spain* decision.[141] As noted above, this included strict limits on notice to publishers, and expansive extraterritorial application. It emphasizes the CJEU's statement that the data protection rights of an individual shall prevail over the economic interests of the search engine operator and the interests of the Internet users to obtain information through the search engine. This is due to the significant impact of data processing on the fundamental right to privacy. However, the sensitivity of the processed data and the public interest shall be taken into consideration during this assessment. It opines that "[t]he impact of [RTBF de-listings] on the freedom of expression of original publishers and users will generally be very limited," both because of the public interest balancing exercise Google is supposed to conduct and because de-listed content will still be available on the Internet.[142]

The French Data Protection Authority has raised a claim for Google to de-list results everywhere in the world, not just on European domains raising issues of extraterritorial application.[143] This interpretation of the RTBF raised significant concerns worldwide about justification of such implementation of the RTBF and its effect on the right to freedom of expression.[144] Google appealed the decision of the French Data Protection Authority requiring search results to be de-listed worldwide before the highest administrative court in France, the Conseil D'Etat.

The issue of notification to publishers came to renewed attention in September 2016, when the Spanish DPA fined Google 150,000 Euros for notifying webmasters about RTBF de-listings.

---

[138] European Privacy Requests for Search Removals (https://www.google.com/transparencyreport/removals/europeprivacy/ [https://perma.cc/63VC-E9XU]). The described statistics are taken on March 6th, 2017.

[139] Microsoft Content Removal Requests Report, https://www.microsoft.com/about/csr/transparencyhub/crrr/ [https://perma.cc/7LY3-XB45]. Google Transparency Report, https://www.google.com/transparencyreport/removals/europeprivacy/ [https://perma.cc/GXN7-TTXY].

[140] The Article 29 Data Protection Working Party was set up under Article 29 of Directive 95/46/EC. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC

[141] Article 29 Data Protection Working Party, *supra* note 127.

[142] *Id.* at 6; Carol Umhoefer, France's Highest Administrative Court Requests a Preliminary Ruling from the ECJ on the Right to be Forgotten, (Mar.13, 2017), http://blogs.dlapiper.com/privacymatters/france-frances-highest-administrative-court-requests-a-preliminary-ruling-from-the-ecj-on-the-right-to-be-forgotten/ [https://perma.cc/8DB4-P5MJ].

[143] Right to de-listing: Google informal appeal rejected (https://www.cnil.fr/fr/node/15814 [https://perma.cc/9672-9TB3])

[144] Global Right to Be Forgotten Delisting: Why CNIL is Wrong, Daphne Keller; Nov.18, 2016 (http://cyberlaw.stanford.edu/blog/2016/11/global-right-be-forgotten-delisting-why-cnil-wrong [https://perma.cc/B8P7-3M3Z]); *See generally*, Kate Tummarello, *We Won't Let You Forget It: Why We Oppose French Attempts to Export the Right to Be Forgotten Worldwide*, EFF, (Nov. 29, 2016), https://www.eff.org/deeplinks/2016/11/we-wont-let-you-forget-it-why-we-oppose-french-attempts-export-right-be-forgotten [https://perma.cc/QSE8-CEX8]

The case is currently being appealed to the Spanish courts.[145]

Finally, new developments have arisen before the CJEU itself. In the *Manni* case, the court held that a data subject could not compel a public registry of companies to delete or restrict access to information about a corporate bankruptcy with which he had been associated. The court noted that individual EU countries could, but did not have to, permit restriction of access to such data in limited circumstances.[146] Another case, recently referred to the court from France, examines Google's processing of "sensitive" personal data such as health information.[147]

There are various cases in Europe applying *Google Spain*, and the variety of interpretations of the concept is evident. For example, a recent decision of the Court of Rome in Italy reportedly favors the right of freedom of expression.[148] An attorney in Italy requested de-indexation of fourteen links identified via a search of the attorney's name. The Italian Court rejected the claim based on three factors: a) search results may not be removed if they are recent and relevant, b) the information is of public interest, and c) the public involvement of the plaintiff.

A similar case was filed in the UK based on the RTBF, where a man has been sentenced to several years in jail for committing a crime involving the public revenue.[149] He requested that several prominent media organizations and Google remove articles about him. The Nottingham County Court rejected the application because the article is of "significant public interest" and because the individual is still serving his sentence (i.e. the statements published in the articles are not yet outdated).

Another important development in the EU is the passage of the EU General Data Protection Regulation ('GDPR'), which will enter into force on May 25, 2018. This legislation had been in the works well before *Google Spain*, when the EU realized that the digital era and the increased processing of personal data required a uniform approach between EU Member States in relation to personal data protection.[150] In contrast with the 1995 Data Protection Directive, the GDPR

---

[145] Miquel Peguera, *Derecho al olvido: ¿el buscador puede informar a la fuente de la eliminación de un enlace?*, Responsabilidad en Internet, (Mar. 14, 2017), https://responsabilidadinternet.wordpress.com/2017/03/04/derecho-al-olvido-el-buscador-puede-informar-a-la-fuente-de-la-eliminacion-de-un-enlace/ [https://perma.cc/7TKW-QJWU]; David Erods, *Communicating Responsibilities: The Spanish DPA Targets Google's Notification Practices when De-listing Personal Information*, https://inforrm.wordpress.com/2017/03/21/communicating-responsibilities-the-spanish-dpa-targets-googles-notification-practices-when-delisting-personal-information-david-erdos/ [https://perma.cc/4TEJ-7EDB].

[146] C-398/15, Camera di Commerio, v. Salvatore Manni, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=188750&occ=first&dir=&cid=526051 [https://perma.cc/4DPB-9C6M].

[147] *FRANCE: France's Highest Administrative Court Requests a Preliminary Ruling from the ECJ on the Right To Be Forgotten*, Privacy Matters: DLA Piper, (March 13, 2017) http://blogs.dlapiper.com/privacymatters/2017/03/13/ [https://perma.cc/E5GC-BJDF].

[148] Right to be Forgotten, Right to Reputation and Privacy: Comment to the Decision No. 23771/2015 of the civil court of Rome, http://www.lexology.com/library/detail.aspx?g=99d62f78-4eb1-4de7-8661-98c646d943f0.

[149] Man loses "right to be forgotten" Google court bid-BBC news, BBC News, http://www.bbc.com/news/uk-england-nottinghamshire-33706475 [https://perma.cc/ZUE4-V3QG].

[150] European Commission - Press release: "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, http://europa.eu/rapid/press-release_IP-12-

expressly references the "RTBF" and, similar to the approach of the European court, aims to balance the RTBF[151] with the right to freedom of expression.[152] However, the GDPR has been criticized for establishing substantive rules that inadequately protect free expression, as well as introducing new notice and takedown processes that are less favorable to free expression than prior laws.[153] It remains to be seen whether the newly envisaged RTBF will clarify the pending issues following the *Google Spain* judgment or give rise to further uncertainty.

C. How Can RTBF Be Seen Under The ACHR?

This section analyzes the EU-based concept of RTBF in the context of the OAS human rights framework. Our intention is to highlight the most relevant elements of the RTBF against the ACHR standards, as these have been understood by its interpretative bodies. We find considerable tension between OAS free expression standards and the RTBF as adopted by the CJEU.

As discussed in the previous section, the exact boundaries of the current RTBF concept are evolving. Taking the *Google Spain* decision as the defining moment for this doctrine, we have identified four inflection points at which the RTBF challenges existing safeguards in international human rights law:

a) Are search engines "data controllers" for indexed content[154] and, if they are, how should they comply with RTBF requests (deletion, general de-listing, de-listing in relation to personal data)? ("the definition of RTBF");
b) What standard is required to be shown to make a RTBF request, and what public interest concerns offset this standard (i.e., how the "irrelevant, inadequate" standard articulated in Europe would apply under the OAS framework)? ("the standard of RTBF");
c) Who is best placed to determine whether a RTBF applies in each case (i.e., the search engine, an independent agency or a court)? ("the RTBF decision-maker"); and
d) What procedural safeguards should be put in place in addressing RTBF requests (for example, should the publisher or webmaster be notified and allowed to object)? ("the procedure of RTBF").

In the following subsection, we frame our analysis by presenting the dominant views raised for and against the RTBF. We then highlight the existing safeguards within the International, EU and OAS human rights framework for freedom of expression and privacy and data protection, focusing on the substantive and procedural rights/safeguards therein. Finally, subsection C(3), analyses the main elements of the RTBF, as described in section B, to understand how they relate to the ACHR safeguards and interpretations.

46_en.htm [https://perma.cc/YUX9-6LBH].

[151] Article 17, para 1 & 2.

[152] Article 17, para 3.

[153] Daphne Keller, The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation (2017) (forthcoming, Berkeley Tech. L. J.), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914684 [https://perma.cc/SF4Q-F22P].

[154] Note that this question is distinct from asking whether search engines act as controllers for user data that they collect and store in accounts, logs, advertising profiles, or similar back-end storage systems.

1. Conflicting Views Around The RTBF

According to its defenders, the RTBF is a critical tool to address the problem of the widespread availability of information that may damage or affect someone's reputation through the Internet.[155] Rather than a new right, many see it as a new doctrine whereby the existing fundamental right to the protection of personal data can be exercised on the Internet -- much as it had been against more traditional data controllers like banks, telemarketing companies or credit score agencies.[156] Following this argument, just as an individual is capable of requesting the removal of his name or address from a backend database, he or she should be able to request a search engine to stop using his or her personal data as a particular search result.

Those who oppose the RTBF as prescribed by the European authorities believe that it creates a great risk for freedom of speech and information.[157] They argue that allowing any individual to request the deletion of a search result in connection with her name opens the door to a form of private censorship sanctioned by the government. An individual's right to control the information that is publicly linked with their name is placed in direct opposition to the public's right to seek and impart information, or in the search engine's right to free expression in the form of accurate and complete search results.[158]

The potential conflict between these rights is particularly pronounced in the context of the Internet which, while providing an important mechanism for free speech, also has the potential to erode an individual's privacy and reputation on a large scale by allowing unfettered dissemination of information.[159] While some commentators do not deny that with the widespread availability of personal data, harmful information or defamatory content is a real problem online, they believe that the RTBF or a data protection legal framework is not the right tool for addressing the issue.[160]

The RTBF also raises questions regarding who is best placed to resolve this conflict between privacy and the freedom to receive and impart information: intermediaries, administrative agencies or national courts. Outsourcing RTBF decisions — and the function of balancing privacy and freedom of expression rights — to intermediaries causes particular concern.[161] Intermediaries are commercial entities whose fear of potential liability, or lack of resources to fully address requests for de-listing, may motivate an overzealous response to individual requests that

---

[155] *See*, among others, Eric Posner, We All Have the Right to Be Forgotten, SLATE (May 14, 2014), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html [https://perma.cc/GM5T-TAEN].

[156] *See generally* Keller, *Europe's Right to be Forgotten in Latin America, supra* note 103.

[157] Danny O'Brien & Jillian C. York, Rights That Are Being Forgotten: Google, the ECJ, and Free Expression, ELECTRONIC FRONTIER FOUNDATION (July 8, 2014), https://www.eff.org/deeplinks/2014/07/rights-are-being-forgotten-google-CJEU-and-free-expression [https://perma.cc/KNH5-6EZY].

[158] *See generally*, Eugene Volokh and Donald M. Falk, Google: First Amendment Protection for Search Engine Search Results (April 20, 2012), http://volokh.com/2012/05/09/first-amendment-protection-for-search-engine-search-results/ [https://perma.cc/RR4T-SKQA].

[159] *See* UNESCO, Privacy, Free Expression and Transparency (2016).

[160] Jonathan Zittrain, "Don't Force Google to 'Forget,'" *The New York Times*, May 14, 2014, https://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html [https://perma.cc/4SP7-V9CN].

[161] See, eg, UN Freedom of Expression at 104-105; House of Lords Report on RTBF at para 36.

information be de-listed,[162] leading to a chilling effect on free speech.[163]

This aspect of the debate around the RTBF appears to be about means and not ends. Both sides may agree that some legal or technological solution should exist to address the issue of the unlawful use of personal data online, but they diverge on key questions such as whether erasure obligations should lie with search engines, who provide access to information already published, or directed exclusively to those who publish it; as well as whether data protection laws provide the best legal framework for balancing the rights in issue.

These conflicts are particularly pronounced in the context of OAS human rights framework with the ACHR's broad scope for freedom of expression relative to other rights.[164] The following subsection describes the main human rights guarantees applicable to the rights in debate in the RTBF.

2. The RTBF and International Human Rights Instruments

This section highlights the key criteria in international human rights instruments that inform the conversation about the RTBF, with an emphasis on the ACHR and its interpretive documents. In addition to the general overview of intermediary liability discussed in Part II.B, RTBF in particular raises concerns about the balance of privacy with free expression, and about the role of search engines in supporting or burdening Internet users' rights.

a) International and European Human Rights Framework

The RTBF broadly poses a conflict between privacy and free expression rights. Supporters of the RTBF see it as a manifestation of the universal human right to privacy under Article 17 of the ICCPR. In 1988, the UN HRC, in General Comment 16, identified a particular right for individuals to ascertain which public or private bodies control files about them, and "[i]f such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law… to request rectification or elimination."[165]

Data protection aspects of the privacy right are uniquely significant within the EU legal system, because of the express inclusion of data protection as a fundamental right in Article 8 of in the EU Charter of Fundamental Rights.[166] (By contrast, data protection rights are not listed in the European Convention on Human Rights, although the privacy right under that document

---

[162] Keller, *Europe's Right to be Forgotten in Latin America, supra* note 103 at 17; House of Lords Report on RTBF para 33-35.

[163] UNESCO, Privacy, Free Expression and Transparency (2016) at 104-105.

[164] See, for example, IACHR OSRFE (2010) *supra* note 3 at 102-105. IACHR OSRFE (2013) *supra* note 24 at 14, 24; *see also*, *Belen Rodriguez*, Judgment R.522.XLIX (2014) at para 11-13.

[165] ICCPR General Comment No. 16: Article 17 (Right to Privacy).
The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, at para 10, http://www.refworld.org/docid/453883f922.html [https://perma.cc/LS6C-VES8]; IACHR OSRFE (2013) *supra* note 24 at para 141.

[166] Charter of Fundamental Rights of the European Union, 2000/C 364/01, http://www.europarl.europa.eu/charter/pdf/text_en.pdf [https://perma.cc/8B27-8UWC].

presumably encompasses some aspects of data protection.) The CJEU in Google Spain interpreted the Data Protection Directive "in light of fundamental rights" to both data protection and privacy, but did not address whether RTBF was mandated by fundamental rights considerations.[167]

European human rights instruments also address free expression, and have been interpreted as a source of constraints on intermediary liability. In pre-*Google Spain* guidance, for example, the Council of Europe stated that search engines should not have the obligation to "monitor their networks and services proactively in order to detect possibly illegal content and should not conduct any ex-ante filtering or blocking activity" unless it is directed by a court, and that "de-indexation" should be transparently carried out by public authorities aligned with due process requirements.[168]

Speaking to the balance of rights, the Council of Europe in its Guide to Human Rights for Internet Users[169] states that freedom of expression, the right to information and privacy must be "balanced" and that these rights, on principle, should be respected equally.[170] As UNESCO noted in discussing the RTBF, treading this balance is complex: companies such as Google may receive a host of requests, some illegitimate, which will cover up misdeeds of a politician, and some legitimate requests from parents to de-list names of minors who were victims of sexual abuse.[171] UNESCO's study on Privacy, Free Expression and Transparency finds the effect of the RTBF on access to information may be problematic, saying it is "debatable in the long run if this decision to remove what the court deemed as irrelevant and outdated information strikes the right balance between the two fundamental interests."[172]

b) OAS Human Rights Framework

Bringing a concept like the RTBF into the OAS Region poses a risk of conflict with the OAS human rights framework. The degree of conflict will depend on the interpretation of RTBF at issue in a particular case. As discussed in the introduction, the OAS has been recognized as the human rights framework providing the broadest protections for free expression. Commenting on its predominant role in the OAS human rights framework, the OSRFE has said that any restrictions based on "other international instruments are not applicable in the OAS context, nor should such instruments be used to interpret the American Convention restrictively."[173] More specifically, the

---

[167] *Id.* at para 68-69; *See also Id.* at para 80 (search engine is "liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name") & para. 97 (data subject may "in the light of his fundamental rights" request de-listing); para 58 (denying RTBF obligations for search engines would "compromise the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons").

[168] See Council of Europe, Recommendation CM/Rec(2014) 6 of the Committee of Ministers to member States on a "Guide to Human Rights for Internet Users" available here https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31 [https://perma.cc/XKN6-FYMH] at para 51.

[169] *Id.*

[170] *Id.* at para 41.

[171] Fostering Freedom Online the Role of Internet Intermediaries (2014) (UNESCO Publishing; Rebecca Mackinnon, Elonnai Hickok, Allon Bar, Hae-in Lim) at 118-119.

[172] UNESCO, Privacy, Free Expression and Transparency (2016) at 28.

[173] IACHR OSRFE (2010) *supra* note 3 at p 2.

OSRFE has said in its 2017 Report that "the application to the Americas of a private system for the removal and de-indexing of online content with such vague and ambiguous limits is particularly problematic" to the light of the ample Freedom of Expression protections that exist in the ACHR.[174] This counsels some skepticism about a ruling based on the European Charter. At the same time, the ACHR also recognizes the right to privacy of every individual, and provides standards for balancing that right against the expression and information rights of others.[175]

OAS standards may diverge from European standards both with respect to the substantive balancing of rights, and the procedural requirements to protect those rights in the context of intermediary liability and search engines.

i) Substantive rights: freedom of speech, privacy, data protection

Implementation of the RTBF in OAS countries could not only impact publishers' freedom of expression (and, arguably, the freedom of expression of the intermediary service provider), but also the right of the general public to receive information.

Privacy is a key human right recognized in the ACHR. Article 11.2 says that "no one may be the object of arbitrary or abusive interference with his personal life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation." In the past, this has been interpreted as an obligation of the State to respect the private sphere of the individual and a duty to ensure that third parties do not act in a way that could arbitrarily affect it.[176] In addition, Principle 3 of the Declaration of Principles recognizes a right that appears more similar to the European data protection concept, providing that an individual has the right "to access to information about himself or herself or his/her assets expeditiously and not onerously, whether it be contained in databases or public or private registries, and if necessary to update it, correct it and/or amend it."[177] This Principle refers to the *habeas data* writ.[178] Significantly, and unlike the EU RTBF standard, Principle 3 does not include reference to individuals having any right to erasure.

The OSRFE has discussed this protection, stating that: "Given the impact on the private life of individuals, States should establish systems for the protection of personal data, to regulate their storage, processing, use, and transfer."[179] The OSRFE also noted that states must in some instances require deletion of data "if necessary and proportioned."[180] From this passage, it is clear

---

[174] IACHR, OSRFE, (2017) supra note 44 at 53.

[175] Article 11, ACHR.

[176] IACHR OSRFE (2013) *supra* note 24 at 9.

[177] Principle 3, IACHR's Declaration of Principles on Freedom of Expression.

[178] Background and Interpretation of the Declaration of Principles at para 12.

[179] IACHR OSRFE (2013) *supra* note 24 at 58-64 (citing United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, *Joint Declaration on surveillance programs and their impact on freedom of expression* (June 21, 2013) at [4] https://www.oas.org/en/iachr/expression/showarticle.asp?artID=926&lID=1 [https://perma.cc/5N7C-QJNE]; A/HRC/17/27 at 56.

[180] IACHR OSRFE (2013) *supra* note 24 at 61.

that the interpretation that OSRFE has given to the ACHR allows not only data protection regulation but even the deletion of personal data. However, the OSRFE has warned recently that both the removal of content from the Internet and, to a lesser degree, the de-indexing of content can be seen as clear interferences with the right to freedom of expression as well as the right of access to information, given their information limiting effects.[181] Therefore, where free expression rights are at issue, the clear limit to this deletion can be found in the three-step test and standards established in key OAS human rights documents.

The Declaration of Principles speaks to the balance of free expression and privacy in Principle 10, saying that "privacy laws should not inhibit or restrict investigation and dissemination of information of public interest." In this regard, the OSRFE has later said that the protection of individual privacy "must be based on reasonable and proportionate criteria that do not end up arbitrarily restricting the right to freedom of expression."[182] On the conflict between personal data protections and freedom of speech, the OSRFE has mentioned that it "cannot lead to the imposition of restrictions on information disseminated by media outlets that could affect the privacy rights or reputation of an individual."[183] Principle 10 further establishes an "actual malice" standard for public figures, prohibiting liability for a speaker unless he or she "had the specific intent to inflict harm, was fully aware that false news was disseminated, or acted with gross negligence."[184]

Explicating this protection in its Background and Interpretation of the Declaration of Principles, the OSRFE identified both an "intent" standard and vindication through civil procedure as key elements in balancing privacy and expression or opinion rights. It stated,

> The State fulfills its obligation to protect the rights of others by establishing statutory protection against intentional attacks on honor and reputation through civil procedures, and by enacting legislation to ensure the right to rectification or reply. In this way, the State safeguards the private life of all individuals, without exercising its coercive power abusively to repress the individual freedom to form and express an opinion.[185]

In addition, the explication continued, "[t]here should be no liability when the information giving rise to a lawsuit is a value judgement rather than a factual assertion."[186] As an illustration of this, the right to reply under Art 14 is cited as the first means to address an allegation of unlawful privacy invasion. If this is insufficient, and only if it was shown that serious harm was caused with an intentional or obvious disregard for the truth, civil liability can be imposed on the speaker, in

---

[181] IACHR, OSRFE, (2017) supra note 44 at 53.

[182] IACHR OSRFE (2013) *supra* note 24 at 58.

[183] IACHR, OSRFE, (2017) supra note 44 at 54.

[184] Principle 10, IACHR's Declaration of Principles on Freedom of Expression; Background and Interpretation of the Declaration of Principles at para 46.

[185] Background and Interpretation of the Declaration of Principles. The Background document states that Principle 10 "essentially refers to ... laws created to protect people's reputations (commonly known as libel and slander laws)," but the language of Principle 10 itself refers to "Privacy laws," making clear its application to privacy broadly.

[186] *Id*. at para 47.

accordance with the strict requirements of Art 13.2.[187]

ii) Procedural rights: due process

As noted above, the OSRFE in explicating Principle 10 identified civil court proceedings as a key component in striking a balance between privacy and expression rights. This overlaps with the right in Article 8 of the ACHR to a hearing with due process guarantees before an independent and impartial tribunal. The same emphasis on courts and public adjudication of rights appears in OAS materials regarding intermediary liability and suppression or de-listing of online content. The OSRFE recently said that intermediaries that do not specifically intervene in the unlawful content should not face liability or removal obligations unless they "refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it."[188]

Internet search engines in particular have been praised by the OSRFE as one of the main facilitators of the circulation of information and ideas on the Internet, playing an important role in creating the social dimension of freedom of expression.[189] Their role as intermediaries between publishers and readers, at the same time, has been recognized as a potential choke point for the free circulation of ideas and information online. In the 2011 Joint Declaration, the Special Rapporteurs emphasized the need to shield Internet intermediaries from liability for content created by others as long as they do not exercise editorial control over it.[190]

Human rights sources and the Manila Principles support additional, more specific procedural rights, including the provision of notice to the publisher when content is restricted, and an opportunity for the publisher to contest the restriction.[191] Article 25 of the ACHR requires the right to simple and prompt recourse from a competent court or tribunal for any alleged violation of fundamental rights. Both UN Special Rapporteur and the OSRFE have established previously that any person affected by measures that restrict freedom of expression "as a result of the decisions of intermediaries should have, depending on the specific domestic regulations, legal remedies to contest such decision and mechanisms for reparations in the event of the violation of their

---

[187] Art 13.2 provides that any restriction of free expression must be expressly established by law to the extent necessary to ensure respect for the rights or reputations of others, or for the protection of national security, public order or public health and morals. IACHR OSRFE (2010) *supra* note 3 at 79. *See also*, Frank La Rue writing for the Google Advisory Council, "The Advisory Council to Google on the Right to be Forgotten," Final Report, February 2015, available at: https://www.google.com/advisorycouncil/ [https://perma.cc/434G-DLWF].

[188] Joint Declaration on Fake News. The earlier OSRFE report similarly stated that "an order to include or remove specific links, or the imposition of specific content in Internet publications" was a form of "prior censorship" according to the case law of the OAS human rights framework and in violation of Article 13. IACHR OSRFE (2010) supra note 3 at 53. The statement refers to a case regarding a film, "The Last Temptation of Christ" I/A Court H.R., Case of "The Last Temptation of Christ" (Olmedo-Bustos et al.) v. Chile. Merits, Reparations and Costs. Judgment of February 5, 2001. Series C No. 73.

[189] IACHR OSRFE (2013), *supra* note 24 at 19.

[190] 2011, Joint Declaration, Section 2.a.

[191] Manila Principle II(a). *See* A/HRC/17/27 at 40; IACHR OSRFE (2013) *supra* note 24 at 39-44; UNESCO, *Privacy, Free Expression and Transparency* (2016) available at http://unesdoc.unesco.org/images/0024/002466/246610E.pdf [https://perma.cc/YP3T-CCDR] at 104-106.

rights."[192] The OSRFE has also previously recommended non-judicial domestic remedies as a way of expediting the resolution of conflicts between users and intermediaries, where users wish to contest the decision of intermediaries to remove their content.[193]

3. Analyzing the EU RTBF Elements Under the OAS Human Rights Framework

In the form articulated by the CJEU, a RTBF that forces search engines to consider and implement the requests to de-index search results based on data protection law would likely amount to a form of information restriction if applied in the OAS region. Not all forms of information restriction are considered censorship or prohibited under the ACHR, however. This section centers on this question and examines the EU RTBF in light of free expression protections within the OAS human rights framework.

As set out in our introduction, under the ACHR, the right to freedom of expression is absolute, unless the restriction is:

1. defined in a precise and clear manner by a law, in the formal and material sense
2. designed to serve compelling objectives authorized by the ACHR; and
3. necessary in a democratic society to serve the compelling objectives pursued, strictly proportionate to the objective pursued, and appropriate to serve such compelling objective.

We now consider the key elements of the RTBF that we highlighted in discussing *Google Spain*: the definition of the RTBF (search engine as controller with de-listing, not deletion, obligations), the appropriate standard of RTBF ("irrelevant" v. "unlawful"), the appropriate decision-maker for RTBF (who should decide on the requests), and the procedure of RTBF (what process is necessary for intermediary removals) within the parameters of an acceptable restriction on free expression under the OAS human rights framework. While aspects of the elements identified in the EU-based concept of RTBF may in some cases be permissible within the OAS region, this concept cannot be automatically transplanted within the OAS human rights framework.

a) The Definition of the RTBF

The EU ruling concluded that Google's search service acted as a controller of indexed content under data protection law, and that the company had de-listing obligations as a result. This interpretation of the Data Protection Directive was not shared by the Court's Advocate General, who recommended the opposite outcome. Behavioral evidence suggests that the Court's interpretation was not so widely held or relied upon prior to the ruling -- otherwise at least some part of the current flood of RTBF litigation and de-listing requests would have started before 2014.

Under OAS standards, this debatable interpretation of the Data Protection Directive might not pass muster. In order for any restriction on speech to be implemented under the OAS human rights framework, such a right must be established in law "expressly, restrictively and clearly."[194] In other words, the law must be drafted in the clearest way possible so that the public is absolutely

[192] IACHR OSRFE (2013) *supra* note 24 at 53.

[193] *Id.*

[194] IACHR OSRFE (2010) *supra* note 3 at 24-25.

certain of its obligations under law.[195]

In addition, the broader human rights framework that guides interpretation of data protection statutes in OAS states may dictate a different outcome. As noted above, the ACHR does not contain an enumerated data protection right like the one in the EU Charter, and the *habeas data* right of Principle 3 does not expressly extend to erasure of data. So, the human rights framework of privacy and data protection would not push as strongly as the EU's did toward designating search engines as controllers. The ACHR's strong free expression rights would further counsel against an interpretation of data protection law that effectively makes search engines responsible for adjudicating the balance of privacy and free expression rights -- an outcome that the OSRFE has consistently warned against in other areas of law.

b) The Standard of the RTBF

The CJEU applied the RTBF to information that is "inadequate, irrelevant or no longer relevant or excessive" – a standard that may be difficult to reconcile with the OAS human rights framework. In the OAS, ACHR Article 11 prohibits "arbitrary or abusive interference with ... private life[.]" This means that laws protecting individual privacy "must be based on reasonable and proportionate criteria that do not end up arbitrarily restricting the right to freedom of expression."[196] As OSRFE has said, "the right to privacy must yield to freedom of expression when the facts disseminated can have public relevance."[197] The threshold for raising a violation of a privacy right under the ACHR thus appears to be higher than the "inadequate or irrelevant" standard described by the CJEU, particularly as the CJEU's standard can compel de-listing even for truthful information and information that does not prejudice or harm the data subject.

While the CJEU standard carves out public information, and in particular says that some information about public figures need not be de-listed, it does not appear to strike the same balance as the "actual malice" standard for privacy rights of public figures in the Declaration. In establishing de-listing obligations for Google, the CJEU nowhere suggests that the search engine meets the OAS 'actual malice' standard, which requires intent, knowledge of falsity, or negligence regarding statements about public figures.[198]

c) The Decision-Maker of the RTBF

The CJEU's designation of search engines as the initial decision-makers in the RTBF context appears in conflict with free expression and due process rights[199] under the ACHR. If the European RTBF were directly implemented in the OAS region, search engines would be tasked

[195] *Id.*

[196] IACHR OSRFE (2013) *supra* note 24 at 58.

[197] IACHR OSRFE (2010) *supra* note 3 at 113.

[198] Background and Interpretation of the Declaration of Principles.

[199] Article 8, ACHR.

with determining alleged violations of privacy rights[200] as well as in respect of the original publisher's free expression and the public's right to receive information[201]

This allocation of removal decisions to private companies – not impartial or independent authorities – contravenes repeated statements, under OAS standards, that intermediaries should not remove content without court adjudication.[202] On this issue, the OSRFE has made clear that "[r]equiring [intermediaries] to conduct a quasi-adjudicatory exercise that weighs the rights of their users exceeds the scope of their competence and could create and encourage abuses against freedom of expression and access to information." Even under more flexible standards permitting some "adjudication" by intermediaries, like that adopted by the Argentine Supreme Court in *Belen Rodriguez*, the EU RTBF appears problematic because it puts search engines in charge of difficult decisions about content that is not plainly illegal.[203] For the reasons set out above, search engines are not disinterested or impartial in responding to takedown requests, and may implement RTBF requests to avoid liability.

d) The Procedure of the RTBF

The existing procedure for the RTBF in Europe does not appear reconcilable with due process protections or with the three-step test for a legitimate restraint on free expression developed in the OAS human rights framework. Most notably, as the RTBF has been interpreted in Europe, there is no requirement to notify the webmaster or the original publisher that their content has been de-listed from Google. The RTBF procedure based on data protection law is simply not designed to allow the participation of interested third parties beyond the data controller and the data subject. Indeed, the Article 29 Working Party's interpretation has been that there no legal basis under EU data protection law that "obliges search engines to communicate to original webmasters that results relating to their content have been de-listed" because that notification in itself would be a new and different unauthorized processing of personal data.[204] Spain's DPA recently affirmed this standard, fining Google for notifying publishers about de-listings. The procedure for RTBF de-listings under the EU's pending data protection law, the GDPR, similarly does not require notice to webmasters and introduces additional problematic procedures.[205]

In contrast, a decision by the Court of Appeals for the First Region in Mexico vacated a Data Protection Agency order to de-list precisely because the Mexican Court considered that the freedom of expression of the original publisher would be harmed without a proper opportunity to

[200] Article 11, ACHR.

[201] Article 13, ACHR.

[202] See discussion *supra* Part I.C.2.

[203] *Belen Rodriguez,* Judgment R.522.XLIX (2014). The Supreme Court gives the examples of child pornography, data that facilitates or instructs the commission of a crime, threatens human life or physical integrity, expresses approval of genocide (among others) as well as harmful content that is detrimental to honor, or contains notoriously false images which in a clear and unquestionable manner, seriously violate privacy.

[204] Article 29 Data Protection Working Party, *supra* note 127 at 10.

[205] Daphne Keller, *supra*, note 153.

be part of the proceedings and exercise his right to audience.[206] Ensuring that publishers and other potentially injured parties can contest de-listing decisions reduces the likelihood that improper RTBF requests will succeed in suppressing lawful speech. It is also consistent with ACHR Article 25(2), which provides that State Parties must ensure that persons claiming legal remedy shall have their rights determined by a competent authority provided for "within the legal system of that state."

D. Thematic Findings and Trends

National law developments that inform our analysis are listed in more detail in the Appendix to this Report. In addition to the European developments discussed above, the following are noticeable developments around the world:

- Argentina, which has what has been called the "most complete" data protection law in Latin America,[207] is considering legislation modeled on the new EU GDPR.[208] Most probably, countries seeking to reach the certification of "adequate level of protection" will choose to adapt their national data protection laws to the same high standards.
- A Canadian court ruled in 2017 that Canadian data protection law applied to content on a Romanian website.[209] Its injunction prohibited publication of Canadian court records on the site, and anticipated that the applicant would use the order in seeking de-indexation by search engines.[210]
- The Colombian Constitutional Court interpreted its data protection law as requiring a news website to update (but not delete) an old news story discussing the victim of a crime, and prevent search engines from indexing the story. In dicta, the Court rejected the Google Spain outcome, stating that to hold search engines liable for the content would be "unnecessary sacrifice of the Network Neutrality principle and, with it, of the freedom of information and expression."[211] Perhaps inadvertently, the court ordered the news website to implement more far-reaching de-listing than resulted from the Google Spain ruling. By requiring the site to use robots.txt or other technical means to prevent the page from being indexed, it effectively took the page out of search results completely -- not only for searches on the plaintiff's name.
- An appellate Court in Mexico ruled that the Mexican DPA improperly ordered Google to de-list results, because the affected publisher was not given notice and an opportunity to

---

[206] Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región, Amparo en Revision 74/2012 (Jul. 7, 2016), http://sise.cjf.gob.mx/SVP/word1.aspx?arch=1100/110000001885932400001001.docx_0&sec=_Mercedes__Santos_Gonz%C3%A1lez&svp=1 [https://perma.cc/N8LW-9ZBZ].

[207] Edward L. Carter, *Argentina's Right to be Forgotten*, 27 Emory International Law Review 23, 33 (2013).

[208] *See* Pablo A. Palazzi, *New Draft of argentine Data Protection Law Open for Comment*, (Feb.8, 2017) https://iapp.org/news/a/new-draft-of-argentine-data-protection-law-open-for-comment/ [https://perma.cc/VLL8-NX3T].

[209] A.T. v. Globe24h.com (2017) FC 114.

[210] *Id.* at para 86. (The Office of the Privacy Commissioner of Canada submitted that this was the most "practical and effective way" of mitigating the harm to individuals.)

[211] Constitutional Court of Colombia, SENTENCIA Nº T-277, Gloria v. Casa Editorial El Tiempo. (May 12, 2015). https://karisma.org.co/wp-content/uploads/2015/07/TUTELA-EL-TIEMPO.pdf [https://perma.cc/KF4Q-VW6S].

contest the order.[212]

- In a troubling Peruvian case involving police investigation of a former public servant, the DPA held that Google was a data controller and initially ordered it to block any search result connecting the data subject with the investigation.[213] On administrative appeal, the DPA required Google to de-list 16 specified URLs but relieved the search engine of the obligation to proactively find and block other URLs -- a key change, given the OSRFE's recent affirmation that "content filtering systems which are imposed by a government and which are not end-user controlled are not justifiable as a restriction on freedom of expression."[214]

Drawing on these and other developments reviewed, we have identified the following trends:

1. Inconsistent Application of the RTBF

We have observed an inconsistent approach to dealing with removal requests from search engines within or outside the OAS region. In some cases, like in Colombia, Courts have not made the search engine liable for data processing activities.[215] In other OAS countries, like Peru, authorities had established that the responsibilities of the search engines include honoring removal requests from users.[216]

Among the countries that adjudicated the cases under data protection laws, like Peru or Mexico, the degree to which this regulation has been applied to search engines has been different. Sometimes it has been interpreted to impose on search engines the general mandate of de-indexing any search result associated with a case (Peru), in others it has been limited to requiring search engines to de-list a particular search result subject to due process for the publisher (Mexico), and in another case it involved ordering a publisher to de-list the content from every search engine (Colombia).[217] In some OAS countries, such as Peru, applying data protection laws to require search engine de-listing expanded on already existing practices of applying data protection law to primary publications, and requiring erasure of data there.[218] In countries such as India where there are no data protection laws and privacy arguments are based on constitutional law, different courts in the country have taken different views, as there are no established grounds that the court can rely on.

---

[212] Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región, *supra*, note 206.

[213] Dirección General de Protección de Datos Personales. Directorial Resolution No. 026-2016-JUS. March 11, 2016. http://hiperderecho.org/wp-content/uploads/2016/06/datos_personales_google_olvido_2.pdf [https://perma.cc/B6DR-65XS].

[214] Joint Declaration on Fake News.

[215] See *infra* Appendix A.1.e.

[216] See *infra* Appendix A.1.h.

[217] In the case of Colombia, the decision was effectively more drastic that the one envisioned by the ECJ since it involved removing the search result from every kind of search query, not just the ones with the name of the claimant.

[218] Paola Nalvarte, *Ojo Público: Law on Personal Data Protection should not be used to censor journalists in Peru*, Knight Center for Journalism in the Americas Blog (August 3, 2016), https://knightcenter.utexas.edu/blog/00-17330-ojo-publico-law-personal-data-protection-should-not-be-used-censor-journalists-peru [https://perma.cc/4VU7-PDQF].

This reveals that the RTBF is still a developing concept. Court conclusions may vary depending on the set of rules they are interpreting, their previous knowledge about how the Internet works and the nature of the story or the information that the individual is seeking to remove from the Internet. This indeterminacy also signals a great opportunity to debate this question under an open and equilibrated human rights framework of analysis that takes into account freedom of expression, freedom of information, due process of law and privacy.

2. The Analysis Is Shaped by the Legal Framework Used

The way in which a case is decided will change greatly if it is analyzed within a data protection framework or, alternatively, outside of it. When data protection is not the governing framework, courts are likelier to closely consider established limits grounded in human rights, constitutional law, or doctrines such as defamation. The data protection concepts of data controllers and data processors seem less flexible to analyze the activities of intermediaries who, through automated processes, deal with vast amounts of information (including personal data) originally published by third parties. In cases applying data protection law, the decision to update or remove a search result is often more narrowly based on an assessment of whether the data is "inexact, incomplete or no longer necessary." This trend includes the decisions analyzed from Mexico and Peru, where data protection authorities determined that the search engine was a data controller and therefore was compelled to accept requests for personal data removal.

In contrast, when a claim is analyzed outside of the data protection framework, it is possible for courts to draw from Constitutional safeguards, liability theories under tort law, and any other statute applicable to the Internet. In those cases, the question is not only about the information but the analysis also includes who published the information, under what circumstances, what outcome is the least restrictive of rights, and what is most effective to resolve the issue. These questions were relevant to the decision in Brazil, where the analysis by courts took place under a broader legal perspective and was informed by human rights law in dismissing claims against Internet intermediaries. However, the lack of a strict frame of reference to address the RTBF can also be a threat to human rights, introducing ambiguity and unpredictable outcomes, as has been the case in some cases in Asia.[219]

3. Increasing assertion of RTBF requests in OAS countries since *Google Spain*

OAS countries have seen a number of RTBF claims, which in some cases have reached high courts. In countries that had a pre-existing data protection law, the CJEU decision in *Google Spain* seems to have particularly encouraged claims based on that case's rationale. The original claims of petitioners in Mexico, Peru and Chile (which does not have a data protection law) refer explicitly to the *Google Spain* decision as grounds of their claim. From this perspective, many plaintiffs have even gone beyond the specific ruling of the *Google Spain* Case in filing their motions. Before this wave of decisions under the RTBF, the natural path for those plaintiffs would have been filing a lawsuit under defamation, habeas data, or tort law. However, given that under those causes of action the law would provide ample opportunity to dispute the veracity of the claim

[219] *See, eg*, India discussed *infra* Appendix A.2.c.

or the scope of damage and would be first adjudicated before a Court, many would-be plaintiffs appear to be turning now to data protection law for a substitute that can give them the same effects with a lower burden of proof.

4. Analysis Under Data Protection Law Is Potentially Incomplete

The *Google Spain* judgment resolved several highly ambiguous provisions of European law. As discussed above, even the CJEU and its own Advocate General reached strikingly different conclusions on key questions. These included the fundamental question whether Google acted as a data controller for indexed content, as well as the viability of "RTBF" erasure requests under EU law. The *Google Spain* ruling has been supplemented in the EU with extensive and careful supporting documents and opinions from groups like the Article 29 Working Party.

By contrast, Latin American courts have not necessarily been so careful in determining key questions such as controller status, or in detailing the parameters of RTBF obligations. Some authorities in Latin America appear to have directly imposed the CJEU's interpretation of the Data Protection framework to search engines, without considering of potential differences under non-EU law or taking into account other legislative protections to the dissemination of information on the Internet. This has led to successful judicial challenges (México) or serious uncertainty about how search engines must proceed to fill in their role as data controllers (Peru). In the countries where some type of RTBF has been recognized by data protection authorities, lack of legal clarity could lead search engines to de-list lawful content.

5. Journalism and the RTBF

We found several cases filed directly against publishers like newspapers, official bulletins and judicial archives, among others, and not against search engines under data protection laws.[220] In a way, this set of cases can be seen as part of an expanding understanding of the RTBF. This trend could have been emphasized by the misnomer of "The RTBF" as it implies the grant of a certain kind of forgiveness or a "second chance" for a person in the face of public opinion. However, most modern data protection laws have an exception for the activities of journalism and media activities, establishing strong limits on their application to those activities. This exception acknowledges that, if the data protection rules were strictly applied to journalism, journalistic activity would be emptied of meaning and social value since they would be subject to objections from any individual.

While this exception strongly protects against direct claims against newspapers and journalism outlets, we have not seen it interpreted by courts to protect (1) the activity by which publishers make their content available through search engines; and, (2) the activity of search engines indexing and linking to those news outlets. There is work to be done in assessing and asserting journalistic organizations' rights with respect to indexation.

In addition, journalistic exceptions should be considered with respect to search engines

[220] *See* discussion of Canada *supra* section A(1)(c), where a complaint was filed against a Romanian website that aggregated public data, in respect of search engines indexing that website.

themselves. Given that search engines exercise very little editorial control over their search results, they could likely not be classified as newspapers or media. However, a second look at the rationale behind the origin of the journalism exception could provide an opportunity to either extend or create a new exemption to other kinds of activities, like search engines "controlling" personal data. Following the same reasoning applied to the journalism exemption, the activities of search engines could be transformed under a close application of data protection laws.

6. Potential Influence of the New European Legislation in the OAS Region

The upcoming GPDR reform in Europe has strengthened protections for the RTBF. As discussed,[221] the GDPR ensures greater consistency between European member states, but imposes stricter notice and takedown procedures which may impact on free expression.[222] The GDPR coming into force in 2018 may cause a wave of influence among other countries of the OAS region, with pressure to adopt its expanded provisions. Argentina is currently considering reforming its data protection laws to reflect the GDPR. These developments should be monitored for consistency with the OAS human rights framework discussed above.

E. Options and Next Steps

The OSRFE should consider several possible options arising from its mandate.[223]

1. Sending information requests to OAS countries to gather information about (1) existing regulation for Internet search engines, including whether they're considered as data controllers for the personal data they make available through search results, (2) how data protection laws, if existing, deal with the activities of online intermediaries for user generated content, and (3) what safeguards exist within their data protection laws for activities protected by freedom of expression and information.

2. Promoting the adoption of national administrative measures to better incorporate free expression protections within DPAs' administrative procedures, such as (1) requiring any RTBF orders to include analysis under national and regional laws on free expression and intermediary liability, and (2) ensuring that attorneys specialized in free expression participate in the DPAs' administrative procedures when considering RTBF requests.

3. Preparing a special report on the impact that data protection laws are having on freedom of speech and issuing interpretive principles grounded in the Inter-American system case law to help national authorities to comply with the ACHR within the scope of their national personal data laws. This is particularly relevant since, beyond RTBF requests, data protection laws may also be used against government's transparency duties.

4. Carrying out promotional and educational activities concerning RTBF and the OAS human

[221] *See* discussion *supra* III.B.2.

[222] Daphne Keller, *supra*, note 153.

[223] IACHR, Mandate of the Office of the Special Rapporteur for Freedom of Expression, http://www.oas.org/en/iachr/expression/mandate/ [https://perma.cc/3GDY-SUKX].

rights framework.

F. Conclusion

This Part reflects the tension between the right to information and freedom of expression and the right to privacy, as reflected in the concept of the RTBF. It also explores the relevance of intermediary liability principles in protecting expression rights. De-listing, or the removal of "irrelevant" information from search engine search results, risks infringing rights to free expression and to receive information. However, this tension is resolved, this debate must be informed by human rights principles.

The OSRFE can promote free expression rights in the context of data protection and RTBF claims through the promotional and educational efforts suggested above; and can prompt national authorities to consider the issue through information requests to individual countries.

PART IV: SITE & SERVICE BLOCKING

A. Introduction

This Part of the Report reviews human rights sources to determine whether orders to block entire websites, applications and/or services are consistent with human rights requirements and, specifically, with the standards of the OAS framework. By reviewing selected cases, decisions, and human rights documents from OAS and other international organizations, our purpose is to identify emerging practices and policy trends, and to assess how they might be treated under the OAS human rights framework.

As the significance of the Internet in enhancing access to information continues to grow, so too have the countervailing forces pursuing the restriction of lawful and unlawful content. One of the possible ways to limit the flow of information is to require Internet Service Providers (ISPs or Access Providers) to implement technical measures blocking content. In some cases, ISPs are ordered to block not only specific content, but also entire websites, applications, or services that contain the content. This extreme and severe measure may be used either for the purpose of censorship, or in the pursue of the legitimate goal of stopping illegal content.

Among other possibilities to restrict the access to information, site and service blocking has become one of the alternatives used by governments and courts (and pursued by private parties) around the world as a cost-efficient means of disabling access to undesired content. Due to the limitations arising from territoriality of laws and the existence of privacy protection/anonymization services on the internet, it is challenging for national governments or private claimants to resolve disputes directly with the speaker or the hosts and intermediaries of "unlawful" content. This has sometimes motivated governments and private parties to target Internet Service Providers to implement site and service blocking (SSB).

Restrictions on entire websites and mobile applications inherently conflict with the objective of promoting free expression online. Indeed, the Inter-American system has emphasized open expression on the internet.[224] Blocking entire sites or applications poses a particularly serious threat to online expression and information rights. Such blocking terminates access to the entire array of information on a site or service — not just to those individual pages, features, or uses that violate the law.

Blocking sites and applications profoundly affects human rights online, especially freedom of expression. The goal of this report is to analyze how OAS human rights law constrains SSB orders. It explores the problems and threats posed to freedom of expression by the use of SSB as a mechanism to remove unlawful content within in a jurisdiction. It conducts a non-exhaustive review of recent developments in OAS countries and elsewhere where websites and internet applications have been restricted (see Appendix A). The objective is to identify patterns and to provide insights into how SSB has been applied in light of existing human rights law and standards

[224] IACHR, OSRFE (2013), *supra* note 24 at 1.

in the OAS system.

Structurally, this section of the Report is divided into six parts including this introduction. The issues raised by SSB are examined substantially in Section B through Section F. Section B defines SSB and discusses the technical means that can be used for implementing such blocks. Section C examines the nexus between human rights and the restriction of online content through blocking orders. This Section highlights the applicability of the ACHR and other international legal documents, the standards agreed upon by the various countries, and the implementation of those standards. Section D highlights trends in the implementation of SSB amongst the OAS countries and generally, around the world. Section E identifies practices that may be implemented to establish minimum safeguards to speakers and users and improve transparency in the exceptional cases where blocking orders are issued, in an effort to reconcile this frequently overreaching measure with the international commitments to protect rights to speech and expression. Section F concludes the document. Appendix A of the Report provides an overview of relevant legal developments pertaining to blocks implemented by national governments in the OAS and discusses significant developments in non-OAS countries.

B. What is SSB?

Site and service blocking orders compel ISPs to completely eliminate users' access to websites or services, including mobile applications. Unless courts have determined that every page or use of the affected material is unlawful, such orders can lead to over-blocking of legal information online. SSB can be imposed based on judicial orders, administrative orders, or private requests.

Efforts to block websites and services are not always intended to restrict freedom of expression. Sometimes restrictions are imposed as a means of ensuring the enforcement of other domestic laws, such as requirements by authorities to have access to the content of communications during an investigation (which have affected WhatsApp) or transit regulation (which have affected Uber). This practice, connected with the sovereignty of countries to regulate the market, may in some cases advance legitimate state interests. In others, it may mask efforts to suppress lawful speech and criticism, hinder the ability of people to self-organize, and prevent intermediaries that enable speech from operating in a determined jurisdiction.[225]

Blocking orders vary widely both in scope and in the technical means used to make content inaccessible. For example, a blocking order can be issued to target a single page within a website, or extend its effects to an entire website or multiple websites. Blocking orders can be easily confused with other enforcement techniques used to restrain internet users' access to content, such as orders to delete content hosted by a specific platform. Thus, a proper distinction between these different techniques is necessary to correctly identify the specific concerns raised by each method and to properly assess their compatibility with freedom of expression and other human rights. This

[225] According to the Organization for Security and Co-operation in Europe (OSCE) report, SSB has also been considered as an option to implement these regional laws due to "the limited effectiveness of domestic laws and lack of harmonization at international level." For more information, *see* Yaman Akdeniz, *Freedom of Expression on the Internet*, Organization for Security and Co-operation in Europe Representative on Freedom of the Media, (2012) at 7, http://www.osce.org/fom/105522?download=true [https://perma.cc/4AY6-UTG8]

section defines SSB and explores the technical methods used to implement blocks.

1. Scope of the Report

As mentioned in the Introduction to this report (Part II), there are many technical means and legal approaches to address the existence of unlawful content on the internet. A properly balanced regime must take into full consideration the dual dimension (individual and collective) of freedom of expression and must not provide excessive incentives for intermediaries to remove content to avoid liability. This Part of the report focuses on orders or requests directed at Internet Service Providers (ISPs or Access Providers), and requiring them to disrupt access to entire services (such as the Linkedin app) or websites (such as www.linkedin.com), disabling the retrieval of any information from those sources.

Broad SSB orders can disable entire services and websites and applications that are used to transmit ideas and expression (such as social networks, messaging apps, or apps that provide access to media and journalistic content). These orders may be issued to address pieces of unlawful content on a website or service, or serve as means to ensure enforcement of domestic regulations. In both cases, these SSB orders can be considered a severe restriction on the free flow of information and raise a number of legal and policy concerns.[226]

This report focuses on blocks that affect entire sites and services, and not on narrower blocks targeting only individual webpages, due to the greater threat they may pose to freedom of expression and other human rights.[227] An example of a blocking measure that affected an entire service with important consequences for the freedom to receive and impart information is the recent blocking of LinkedIn by Russian authorities,[228] which was followed by a later order mandating the removal of the application from mobile app stores.[229] The orders were grounded on the claim that the company failed to comply with a domestic data localization rules, which mandate

[226] From a legal perspective, a number of issues can be raised regarding blocking orders targeting ISPs. Can these intermediaries be requested to provide support to authorities seeking to limit or impede access to a certain type of content? Does the plaintiff or requesting agency need to demonstrate that the intermediary is being effectively used to access or distribute the unlawful content, or is the availability of certain content on the internet enough to justify a blocking order against an ISP? Should a blocking order specify the technical details of the block or leave this up to the intermediary? What are the costs that may be imposed on ISPs for implementing a blocking measures? Is it fair and legal to impose this burden on a private party unrelated to the illegal conduct?
From a policy perspective, other questions can be raised. How do the costs associated with this kind of measure impact the price of service and, consequently, the access to the Internet? Is it a sound policy to push ISPs into the position of supporting enforcement against illegal content? What are the risks associated with this? Once the costs of these measures are absorbed by ISPs and an enforcement framework based on blocking is in place, will ISPs or regulators have incentives to extend the use of blocking measures to include other types of "undesired" content?

[227] An initial approach to such general block suggests it would be hard to accept them under the human rights standards examined in Part II.C.1.

[228] For more information, *See* LinkedIn blocked by Russian authorities, BBC: Technology, (Nov. 17, 2016), http://www.bbc.com/news/technology-38014501 [https://perma.cc/NE5T-PDBM].

[229] Cecilia Kang & Katie Brenner, *Russia Requires Apple and Google to Remove LinkedIn From Local App Stores*, The New York Times, (Jan. 6, 2017)
https://www.nytimes.com/2017/01/06/technology/linkedin-blocked-in-russia.html [https://perma.cc/4VTT-3V77].

that companies store users' data within the Russian territory.[230] Similarly, in 2012 China blocked the entire New York Times website.[231] The practice of blocking a service or application because it does not comply with local rules (in opposition to blocking orders related to unlawful content) has been observed in other countries as well, including in the OAS region. The major case in the region is, probably, the WhatsApp block in Brazil for failing to provide content of communications and other metadata to law enforcement during a local criminal investigation.[232] Uber has faced similar bans or suspensions in many countries based on the finding that it does not comply with local regulations, such as taxi licensing.[233]

In focusing on SSB by ISPs, this report excludes from its scope several other mechanisms for suppressing online content. For example, it does not cover actions that can be taken by content hosting platforms, such as deleting a hosted page or restricting access to users from particular countries. Nor does it cover controls implemented at the user-level, such as browser-based parental controls that restrict children from accessing adult content. And, as mentioned above, it does not address the narrower blocking that an ISP can carry out by denying users access to a particular, individual webpage.

Additionally, this report does not address content filtering. Content filtering[234] is a different and more sophisticated form of blocking that recognizes and restricts particular text, images, or other content, rather than simply imposing a blacklist against particular web addresses.[235] Historically, filtering efforts by ISPs have depended on "deep packet" inspection[236] to recognize and block specific keywords or content, raising important concerns related not only to the protection of freedom of expression, but also to the privacy of internet users.

---

[230] LinkedIn has managed data localization in China in order to comply with national norms. Ingrid Lunden, *LinkedIn is now officially blocked in Russia*, (Nov. 17,2016) https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/ [https://perma.cc/Z6NX-EMXL].

[231] Jethro Mullen, *China blocks New York Times website after story on leader's family wealth*, CNN (Oct.26, 2012) http://edition.cnn.com/2012/10/26/world/asia/china-times-website-blocked/ [https://perma.cc/9KWU-QAGX].

[232] This ban was later removed and held disproportional by the Supreme Court. The case is explained in further detail in Appendix A.

[233] The blocking orders issued against the Uber App/Service fall out of the scope of this report as they do not involve the freedom to seek, receive and impart information as a main concern. However, it is relevant to acknowledge the existence of these blocks, as the same techniques can be utilized to address unlawful content online or to block content or a communication tool under the argument that a service does not comply with local rules. For more information about blocks against Uber, see: http://www.businessinsider.com/heres-everywhere-uber-is-banned-around-the-world-2015-4 [https://perma.cc/X8UC-LPAB].

[234] For more information on filtering and its limits, *See The Limits of Filtering: A look at the Functionality & Shortcomings of Content Detection Tools*, Engine, http://www.engine.is/the-limits-of-filtering [https://perma.cc/2MGT-8YFA].

[235] *See* discussion of blocking and filtering techniques in Christina Angelopolous et. al, *Study of Fundamental Rights Limitations for Online Enforcement through Self-Regulation*, http://www.ivir.nl/publicaties/download/1796 [https://perma.cc/QDM8-347J] at 6-10. UN HRC, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38, (May 11, 2016), 13 http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/38 [https://perma.cc/4N2G-FJYM].

[236] Duncan Geere, *How Deep Packet Inspection Works*, (Apr. 27, 2012) Wired UK, http://www.wired.co.uk/article/how-deep-packet-inspection-works [https://perma.cc/4CAK-MDRT].

2. Technical Methods to Block Sites and Services

The primary technical methods used by ISPs to block access to sites and services are URL blocking, IP blocking, and DNS blocking. The Chancery Division in the UK discusses these and related blocking techniques in more detail in its *Cartier Int'l AG v. British Sky Broadcasting* ('Cartier') decision.[237] It is possible to bypass all three forms of blocking using circumvention tools, but the blocks are effective against the average Internet user.

URL blocking - The Uniform Resource Locator or URL is the user-friendly text address that internet users type into a browser to access a site or a page -- for example, www.wikipedia.org. If an ISP blocks the URL, users can no longer access it by typing the URL on their browser. ISPs can use this technique to block individual pages or, in the cases relevant for this paper, they can use it to block entire sites or domains.

IP Blocking - The Internet Protocol or IP address for each website is the numeric address identifying a site's web server and allowing it to be found by other Internet-connected devices. For example, 91.198.174.192 is the IP address for www.wikipedia.org. A single IP address can correlate to more than one website, so if ISPs block a site's IP address, they may inadvertently block other sites as well.[238]

DNS Blocking - The Domain Name System ('DNS') is a decentralized system used by web browsers to look up the IP address for any given URL. When a DNS block is applied, an ISP alters its DNS records so that a user's search for a domain name does not direct to any IP address, or redirects to a different IP address.[239] As a result, the user does not see the page he or she is looking for. DNS blocking has been criticized as creating security risks.[240]

An important issue to be raised at this point is related to the use of standard encryption for web traffic over HTTPS. This type of encryption is very common and highly recommended,[241] protecting the content and integrity of internet users' communications against surveillance and different types of attacks. This protection enhances trust in communications, which is fundamental to ensure the right to freedom of expression.[242]

---

[237] [2014] EWHC 3354 (Ch)

[238] Angelopolous et al *supra* note 235 at 7.

[239] Agatha M. Cole, *ICE Domain Name Seizures Threaten Due Process and First Amendment Rights*, ACLU, (June 20, 2012) https://www.aclu.org/blog/ice-domain-name-seizures-threaten-due-process-and-first-amendment-rights [https://perma.cc/W7FX-Y4WH].

[240] *Switzerland: Blocking of gambling sites - gambling with human rights*, EDRi, (Mar.22, 2017) https://edri.org/switzerland-blocking-gambling-sites-gambling-with-human-rights/ [https://perma.cc/W4MV-V92H].

[241] *See e.g.* HTTPS Everywhere, EFF, https://www.eff.org/https-everywhere. [https://perma.cc/3FK6-PT2P].

[242] David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (2015) http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32 [https://perma.cc/8HLW-MJ57] at para 16-18. And Geoffrey King, *UN report promotes encryption as fundamental and protected right*, Committee to Protect Journalists, https://cpj.org/blog/2015/06/un-report-promotes-encryption-as-fundamental-and-p.php [https://perma.cc/5SAL-

The increasing use of HTTPS is important for this report because it may make it impossible for ISPs to implement blocking orders that target a specific page. This is because when the communication between the user and the website is encrypted, the intermediary cannot identify which specific page URL the user is requesting -- it only knows the URL for the entire website.

In this situation, orders that mandate the blocking of a specific page may force ISPs to block the entire site instead of the individual page,[243] with serious consequences to freedom of expression. On the other hand, the risk of facing a disproportionate block of an entire website may discourage the use of encryption over HTTPS, making communications less safe for all users.

C. Site and Service Blocking and Human Rights

1. SSB and International Human Rights instruments

This section discusses human rights documents published by international bodies that address SSB. In many cases, the documents address internet content blocking generally without distinguishing between targeted blocks of individual pages, and broad blocks of entire sites, services, or applications. Where this is the case, we identify particular considerations that arise for SSB. These documents help identify the main governing principles for SSB around the world and establish the substantive rights that are violated by illegal SSB.

The documents demonstrate that SSB is more than just a technical issue. It extends to the very human rights concerns that the OAS and the ACHR were created to protect, including freedom of expression, freedom of information, and more.

a) General Human Rights Documents

There are certain instances where blocking of specific content at the ISP level may qualify as a lawfully implemented proportional restriction. However, the UN Human Rights Council in its Comment No. 34 (‘General Comment No. 34’)[244] considered that the blocking of an entire website on the internet is not in accordance with ICCPR Article 19, para 3. The document notes that "permissible restrictions generally should be content-specific", while “generic bans on the operation of certain sites and systems are not compatible with paragraph 3” of Article 19.[245] The same document states that "it is also inconsistent with para 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."[246] Altogether, the assessment provided by the General Comment 34 indicates that there is a strong presumption that SSB is invalid, if not completely impermissible.

UQ4C] (Quoting David Kaye (2016)).

[243] Angelopolous et al *supra* note 235 at 9.

[244] *See* CCPR/C/GC/34, http://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf [https://perma.cc/876X-JFF3].

[245] ICCPR, General Comment No. 34 at para 43.

[246] *Id.*

The former UN Rapporteur on Freedom of Expression, Mr. Frank La Rue, builds upon this idea in his August, 2011 Report. In this document, he notes that any restriction applied to freedom of expression online must comply with international human rights laws, including the three-step test (Part IV.C.2).[247] The rapporteur also emphasizes that "States should provide full details regarding the necessity and justification for blocking a particular website, and determination of what content should be blocked should be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences to ensure that blocking is not used as a means of censorship."[248]

The August 2011 report echoes some of the concerns that Mr. Frank La Rue had previously expressed in his May, 2011 report, where the rapporteur requested countries not only to be transparent about website blocking, but also "to provide lists of blocked websites and full details regarding the necessity and justification for blocking each individual website."[249]

These international human rights documents along with others discussed in the Introduction provide a basis from which one can interpret and assess the documents that OAS member states have drafted and signed.

b) Inter-American Human Rights Standards Applicable to the SSB Debate

In addition to the foundational international human rights documents and declarations discussed above and in the Introduction of this report, there are critical documents that have been written and implemented by OAS member states that speak to the importance of balancing human rights considerations with SSB.

The ACHR provides a basic framework for the Americas to consider SSB issues. Article 13 of ACHR states that "Everyone has the right to freedom of thought and expression," which extends to information on the internet.[250] Article 13 states that signatories shall not engage in "prior censorship," but can impose legal liability if necessary in certain instances. The only exception to the prior restraint prohibition is with regard to the protection of children.[251] The IACtHR has interpreted this to mean that, "Article 13(4) of the Convention establishes an exception to prior censorship, since it allows it in the case of . . . moral protection of children . . . . In all other cases, any preventative measure implies the impairment of freedom of thought and expression."[252]

The OAS Declaration of Principles on Freedom of Expression adopted 13 principles for the protection of freedom of expression. It recognizes in Principle 5 that "prior censorship, direct or indirect interference in or pressure exerted upon any expression, opinion or information

[247] A/66/290 (2011).

[248] *Id.* at 13.

[249] A/HRC/17/27 (2011).

[250] Article 13, ACHR; *see* IACHR OSRFE (2010).

[251] Article 13, ACHR at para 4.

[252] I/A Court H.R., Case of "The Last Temptation of Christ" (Olmedo-Bustos et al.) v. Chile. Merits, Reparations and Costs. Judgment of February 5, 2001. Series C No. 73. para. 70.

transmitted through any means . . . must be prohibited by law."[253]

The IACHR OSRFE (2010) defines the range of activities covered by the right to free expression, including the right to speak, write, disseminate, to produce artistic and symbolic expression, to seek, receive and have access to expression, to access information about oneself, and to possess information.[254] These rights extend to the online environment.[255] It sets forth a presumption that all speech, including speech that is "offensive, shocking or disturbing . . ." is protected by the freedom of expression.[256]

Three documents from the OSRFE are particularly useful in understanding blocks. The first one is the 2011 Joint Declaration, which said that "mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse."[257] This idea has been reaffirmed and further developed in the Office's 2013 Freedom of Expression and the Internet Report cited hereinabove as IACHR OSRFE (2013). The admission of blocking, however, was regarded as exceptional due to the extreme nature of the measure, that should be used only when a content could be considered clearly illegal (war propaganda and hate speech inciting violence, direct and public incitement to genocide, and child pornography). Even in the cases in which blocking orders are targeted at specific content, the OSRFE affirmed that the measure should be "subjected to a strict balance of proportionality and be carefully designed and clearly limited so as to not affect legitimate speech that deserves protection."[258] More recently, the OSRFE has reaffirmed that "restrictions on the operation of websites, blogs, applications ... are permissible only to the extent that they are compatible with the conditions provided for the curtailment of freedom of expression".[259]

The document also affirms that the exceptional measure should be applied only to illegal content that has been clearly and fully identified, and "when necessary to achieve a pressing aim."[260] In any case, there must be safeguards in place to prevent abuses, no ex-ante blocking measure can be accepted, and no blocking can be considered legal when a "competent authority that provides sufficient guarantees of independence, autonomy and impartiality" is not involved.[261]

As observed, the human rights documents analyzed set a very high threshold for a blocking measure to be accepted. To further develop what is necessary to meet this threshold, the next item will present an assessment of how the three-step test can be applied to SSB.

---

[253] OAS Declaration of Principles on Freedom of Expression, http://www.oas.org/en/iachr/expression/showarticle.asp?artID=26 [https://perma.cc/G7HA-8NKX].

[254] IACHR OSRFE (2010) at para 19-29.

[255] 2011 Joint Declaration at 1.a.

[256] IACHR OSRFE (2010) at 10.

[257] 2011 Joint Declaration at 3.a.

[258] IACHR OSRFE (2013) at para. 85

[259] IACHR, OSRFE, (2017) supra note 44 at 38.

[260] IACHR OSRFE (2013) at para. 86

[261] IACHR OSRFE (2013) at para. 87-90.

2. The Three-step Test Applied to Site and Service Blocking

The implementation of SSB measures affects a number of human rights expressly recognized in international law. This section evaluates the legal framework of the OAS with respect to human rights and provides a non-exhaustive summary of how these rights may be compromised by SSB.

As mentioned in the Part II.A.1 of this Report, the applicable framework for evaluating the legitimacy of SSB is the three-step test for limitations on freedom of expression set forth by international human rights documents, and developed by OAS and its interpretative bodies.

Below, we discuss how each step of the test can be interpreted in the context of SSB. Afterwards, we will discuss the substantive and procedural rights that may be violated when a SSB measure fails to meet each step of the three-step test.

Step 1: "The limitation must have been defined in a precise and clear manner by a law, in the formal and material sense"

As mentioned in Part II.C.1 of this report, the interpretation prescribed for the *"clearly and precisely provided for by law"* standard by the ECtHR in *Yildirim* provides useful insights in the SSB context. In this case, the Turkish government issued a SSB order for the entire Google Sites platform because a particular Google Sites webpage insulted the memory of Ataturk, in violation of Turkish law.[262] The ECtHR affirmed a set of important standards related to the definition of the expression "prescribed by law", within the meaning of European Convention on Human Rights ('the Convention') Article 10 § 2.

The ECtHR held that the blocking must have at least some basis in domestic law. Second, the court affirmed that "prescribed by law" does not mean that the mere existence of some legal basis is sufficient, but that it refers also "to the quality of law in question." Third, such law must also be accessible for the person potentially affected by the order," who must moreover be able to foresee its consequences", and the law should be compatible with the rule of law. Accordingly, the ECtHR held that entire blocking order is "inconceivable without a framework establishing precise and specific rules regarding the application of preventive restrictions on freedom of expression."[263] It further emphasizes that this legal framework is essential to control the scope of restriction and to provide foreseeability to allow persons to control their actions.[264]

As the court noted, although the law relied upon by the Turkish courts had stipulated a list of grounds and procedural requirements for requesting a blocking order, "judicial checks on the block on access to web sites [did] not contain conditions sufficient to avoid abuse."[265] In a concurring opinion, one judge provided a detailed list of "minimum criteria for Convention-

[262] Law No. 5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting, http://www.wipo.int/wipolex/en/details.jsp?id=11035 [https://perma.cc/3LHM-GCSS].

[263] *Yildirim* No.3111/10, (2012), ECtHR at para 64.

[264] *Id.* at para. 57.

[265] *Id.* at para. 68.

compatible legislation on Internet blocking measures," including limitations on geographic and temporal scope and protections for free expression rights.[266] Given the similarities between the legal standards set forth in the Convention and the ACHR, the ECtHR provides useful insights to the OAS region, stipulating criteria that may help to exclude overreaching blocking orders.

Around the world, and in the OAS in particular, some of the laws most commonly used to justify SSB include copyright/piracy laws, child pornography laws, libel and slander laws, or insults to public officials (*desacato* laws). While these may provide a legal basis for stating that content is unlawful, many do not go into detail or define the possibility of blocking injunctions against innocent parties such as ISPs; they also do not provide specific rules or restrictions for narrowing the scope of these injunctions. In some high-profile cases, blocking orders affecting freedom of expression do not tackle any specific unlawful content, but are aimed at forcing compliance with local rules or law enforcement requirements. In these cases, sites are blocked based on general powers given to authorities to enforce domestic legislation. This kind of block is particularly likely to fail the first step of the three-step test.

Step 2: "Designed to achieve one of the compelling objectives authorized by the Convention"

The ACHR lists two possible compelling objectives that may justify restrictions on free expression: 1. "respect for the rights or reputations of others," and; 2. "the protection of national security, public order, or public health or morals." These objectives are echoed in the General Comment No. 34 on Article 19 of the ICCPR (2011),[267] which notes that the regulation of speech in a particular public space is permissible in order to achieve these ends.[268] The committee goes on to say that restrictive measures must be content-specific, and that "generic bans on the operation of certain sites and systems are not compatible" with upholding freedom of expression.[269] A SSB order is on particularly shaky ground with Step 2 of the three-step test unless it is able to show that it falls within the scope of the abovementioned permissible restrictive measures.

The 2011 Joint Declaration likewise states that "mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure which can only be justified in accordance with international standards, for example where

---

[266] Section 8 of Turkish law Law No. 5651 - Blocking orders and implementation thereof:

> "(1) A blocking order [*erişimin engellenmesi*] shall be issued in respect of Internet publications where there are sufficient grounds to suspect that their content is such as to amount to one of the following offences:
>
> ...
>
> (2) The blocking order shall be issued by a judge if the case is at the investigation stage or by the court if a prosecution has been brought. During the investigation, the blocking of access may be ordered by the public prosecutor in cases where a delay in acting could have harmful effects. The order must then be submitted to the judge for approval within twenty-four hours. The judge must give a decision within a further twenty-four hours. If he or she does not approve the blocking of access, the measure shall be lifted by the prosecutor forthwith. Blocking orders issued as a preventive measure may be appealed against in accordance with the provisions of the Code of Criminal Procedure (Law no. 5271)."

[267] General Comment No. 34, at para 28 and 29.

[268] *Id.* at para 31.

[269] *Id.* at para 43.

necessary to protect children against sexual abuse."[270] The 2011 Joint Declaration indicates that this prong of the test is deeply ingrained in human rights principles, given that its signatories include the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OSRFE and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information.

Step 3: "Necessary in a democratic society to serve the compelling objectives pursued, strictly proportionate to the objective pursued, and appropriate to serve such compelling objective."

SSB orders may be seen as extreme measures that pose a significant threat to freedom of expression. Accordingly, the "necessary, proportionate, and appropriate" test, as discussed in Part II, limits the use of site-blocking to exceptional circumstances only where procedural safeguards are in place to ensure that the measure is, in fact, necessary and proportionate.

The ECtHR interpreted the "necessary" prong in the *Yildirim* case, and found that the necessity test was not satisfied for the broad blocking order issued in that case. The Court concluded that the interference resulting from the block did not satisfy the foreseeability test, and "did not afford the applicant the degree of protection to which he was entitled by the rule of law in a democratic society."[271] The ECtHR also held that if the affected website is not notified of the content's illegality or that the site is the subject of pending criminal proceedings before the blocking order, it supports the lack of necessity.

For the other two elements (proportionate and appropriate) of Step 3, some relevant jurisprudence is offered by Europe. In the CJEU case *Telekabel Wien GmbH v Constantin Film Verleih GmbH* ('Telekabel'), the court approved an order that required an ISP to block an entire website, but that did not specify the technical means of blocking. The court held:

> [W]hen the addressee of an injunction such as that at issue in the main proceedings chooses the measures to be adopted in order to comply with that injunction, he must ensure compliance with the fundamental right of internet users to freedom of information.
>
> In this respect, the measures adopted by the internet service provider must be strictly targeted, in the sense that they must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting internet users who are using the provider's services in order to lawfully access information. Failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued.[272]
>
> The court also stated that the ISP must take reasonable measures to ensure its actions do

[270] 2011 Joint Declaration on Freedom of Expression and the Internet. at para 3a.

[271] *Yildirim* No.3111/10, (2012), ECtHR at para 67.

[272] *Telekabel*, (2014) E.C.R. I-00000 at para 55 and 56.

not "unnecessarily deprive" persons of their right to access content on the internet.[273]

The *Cartier Intl. v. BSB* (2016)[274] case from UK highlights the proportionality argument and attempts to strike a balance between "on the one hand, the intellectual property rights guaranteed by Article 17(2) of the Charter and, on the other hand, the ISPs' freedom to conduct business under Article 16 of the Charter and the freedom of information of internet users under Article 11 of the Charter."[275] Relying on preceding cases of the same jurisdiction, the Court reiterated the guidance on resolving a conflict between two rights provided under the Charter:

> (i) neither Article as such has precedence over the other; (ii) where the values under the two Articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary; (iii) the justifications for interfering with or restricting each right must be taken into account; (iv) finally, the proportionality test – or 'ultimate balancing test' - must be applied to each.[276]

While this European precedent indicates that orders compelling ISPs to block entire websites are compatible with European regional human rights standards, the same may not be true of OAS standards. Indeed, the OSRFE has in the past strongly condemned a proposed site blocking law. In a joint declaration with the UN Special Rapporteur, the OSRFE characterized the blocking of an entire website as a disproportionate, overbroad means of achieving the objective of stopping online piracy and expressed concern that two bills in the U.S., the Stop Online Piracy Act (SOPA) and the PROTECT IP Act, could "silence a good deal of entirely lawful speech, for example by … allowing for an entire website to be targeted if even a small portion of its content is deemed to infringe."[277]

The test of "necessity" under IACtHR precedent is strict. As the Court has said:

> Given this standard, it is not enough to demonstrate, for example, that a law performs a useful or desirable purpose; to be compatible with the Convention, the restrictions must be justified by reference to governmental objectives which, because of their importance, clearly outweigh the social need for the full enjoyment of the right Article 13 guarantees. Implicit in this standard, furthermore, is the notion that the restriction, even if justified by compelling governmental interests, must be so framed as not to limit the right protected by Article 13 more than is necessary. That is, the restriction must be proportionate and closely tailored to the accomplishment of the legitimate governmental objective necessitating it.[278]

---

[273] *Id.* at para 64.

[274] [2016] WLR(D) 389; This is the final decision in the *Cartier (2014)* case previously discussed.

[275] *Id.* at para 125.

[276] *Id.* at para 126.

[277] 2012 Joint Declaration by the UN Special Rapporteur for Freedom of Opinion and Expression and the IACHR-OAS Special Rapporteur on Freedom of Expression, http://www.oas.org/en/iachr/expression/showarticle.asp?artID=888&lID=1 [https://perma.cc/7TGB-F3PB].

[278] Advisory Opinion Oc-5/85 Of November 13, 1985, Compulsory Membership In An Association Prescribed By Law For The Practice Of Journalism (Arts. 13 And 29 American Convention On Human Rights) Requested By The

Various other human rights documents also define "proportionality" in the SSB context. The 2016 Report of the UN Special Rapporteur states that governments must not "disproportionately interfere with free expression" by "pressur[ing] the private sector" (i.e. ISPs) to "take down digital content" without basis in "validly enacted law."[279] Additionally, the Manila Principles also require that "[a]ny restriction of content should be limited to the specific content at issue" under the applicable order or law.[280]

The human rights documents reviewed for this report identify a number of due process protections that must be provided for when ISPs, ordered by governments or by courts, restrict illegal online content. However, it is more difficult to enforce these elements of due process when an ISP engages in site-blocking on its own. The due process elements and their compatibility with SSB are discussed in the following Section.

3. Due Process Concerns Raised by SSB: Procedural Rights Affected by Blocking Orders and the Manila Principles Standards

Alongside the limits imposed by the three-step test, due process concerns are raised by SSB orders. These concerns are listed and explained in the four categories presented below.

a) Judicial oversight

As mentioned, OAS human rights sources state, and the Manila Principle 2 affirms, that content cannot be restricted without an order by an independent and impartial judicial authority recognizing the material as unlawful within its jurisdiction.[281] OAS countries would likely violate their human rights obligations if they held intermediaries liable for failing to block entire sites or services in cases where no court order has been issued, as this might characterize an indirect interference on freedom of expression, prohibited by Article 13, 3 of the ACHR.

Moreover, in most cases the judiciary is the best-equipped institution to determine whether the particular content at issue has actually violated the law, as well as whether these measures are a necessary, proportionate, and an appropriate response. In states that do not require judicial authorization for SSB, government actors and ISPs may be able to block content directly without the judiciary's legal analysis or oversight.

Obtaining a court order for SSB rather than directing ISPs to do so without court approval may be considered a minimum requirement to comply with human rights law; however, the order itself may still violate the state's human rights obligations if it fails to meet the requirements of the three-step test - for example if it violates principles of due process, including user notifications

Government Of Costa Rica at 13.

[279] A/HRC/32/38, (2016) at 22.

[280] Manila Principle 4 (a).

[281] Manila Principles, http://www.manilaprinciples.org.

and transparency.[282]

b) Notice of restriction to end-users and speakers

Important concerns regarding due process emerge when intermediaries are requested/ordered to remove or block content, as the rights of both the speaker (the creator of the content) and of end-users (the ones seeking for information) are affected.

Different legal approaches have addressed this questions by mandating the intermediary to notify the creator of the content or be transparent to the general public when requested to take down content.[283]

In the extreme situations in which blocking orders can be considered legal and in conformity with OAS human rights framework, additional safeguards should be put in place to protect freedom of expression. A blocking order that passes all other human rights tests should still make public, and require to ISP to convey to end users and speakers, the legal circumstances and claims that support the block.

To ensure the right to recourse (article 25, ACHR) of both to end-users and speakers whose rights have been affected by a blocking order, the information on a block needs to be publicly available and widely accessible.

As discussed in the Introduction, both the OAS human rights framework and Principle 6(f) of the Manila Principles mandate transparency and accountability for content restrictions. In the case of SSB, this includes displaying a notice explaining the what and the why of a restriction when end users attempt to access the blocked content. While no equivalent was found in the Inter-American jurisprudence, a UK court decision has adjudged such a notice to be an important safeguard. In the *Cartier* case, based in a suggestion made by the Open Rights Group in its amicus brief that "the page displayed to users who attempt to access blocked websites should contain further information," the court pointed out that "the page should not merely state that access to the website has been blocked by court order, but also should identify the party or parties which obtained the order and state that affected users have the right to apply to the Court to discharge or vary the order."[284]

The notice of restriction safeguard is extremely important for the exercise of the right to appeal by end-users and speakers, further explained below.

---

[282] *See* IACHR, OSRFE (2013) at para 55-66. The essential requirements to be met by a restriction that may compromise the internet, when considered from a systematic digital perspective, can be summarized as "(1) legal enshrinement; (2) seeking a crucial goal; (3) necessity, suitability and proportionality of the measure for achieving the aim sought; (4) judicial guarantees; and (5) satisfaction of due process, including user notifications." The IACHR Report in para 55-66 establishes that any order that restricts the Internet must meet these requirements.

[283] *See* discussion *supra* Part II.C.2.

[284] *Cartier* (2014) EWHC (safeguards established by courts against abuse have been discussed *infra* Appendix A.2.f) at paras. 262-265.

c) Providing affected parties the right to appeal

Upon issuing the order to block a website or service, the court and the intermediary should consider that the person who uploaded, shared, or generated the offending content is entitled to the opportunity to challenge the legality of the order and to pursue redress. Principle 5 of the Manila Principles requires that governments provide both intermediaries and the user who provided the content right to be heard and the opportunity to appeal against content restriction orders.[285]

The 2016 Report of the UN Special Rapporteur urges improved remedial or grievance mechanisms for Internet users affected by removal of their online expression—meaning that users must receive adequate notice of the site-blocking and an opportunity to contest it. This is also emphasized in the IACHR report on Freedom of Expression and the Internet, which states that the restrictive measure must be accompanied by guarantees of due process and judicial remedy. States have a duty to support transparency and access to an effective remedy.[286]

From an internet user's perspective, the CJEU decision in *Telekabel* addresses the safeguard mechanism for internet users by stating that "the 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."[287] This is an important development on the right to information and fair trial. Based on this interpretation, a court might not grant the injunction due to the lack of opportunity for the targeted/offending website or for general internet users to challenge the decision.[288]

This issue has also been addressed in the UK Court, in the *Cartier* (2014) case. In that decision, despite of considering debatable whether "under English procedural law, users affected by an order once made would be able to apply to discharge or vary it in the absence of an express permission to apply", the court required that "future orders should expressly permit affected subscribers to apply to the Court to discharge or vary the orders."

d) Employing the least restrictive means.

The "least restrictive means" by which a government can respond to or restrict illegal content is defined as "the least intrusive instrument amongst those which might achieve the desired result."[289] In other words, blocking injunctions will employ the "least restrictive means" when they

---

[285] Principle 5 (a) Before any content is restricted on the basis of an order or a request, the intermediary and the user content provider must be provided an effective right to be heard except in exceptional circumstances, in which case a post facto review of the order and its implementation must take place as soon as practicable.
Principle 5 (b) "Any law regulating intermediaries must provide both user content providers and intermediaries the right of appeal against content restriction orders."

[286] IACHR, OSRFE (2013) at para 84-90 and 107.

[287] *Telekabel*, 2014 E.C.R. I-00000, at para 57.

[288] Martin Husovec (2014), *supra* note 92.

[289] General Comment 27 (1999). (The same definition has been adopted in the context of freedom of expression in

are implemented to effectively block the least amount of content possible that would still enable them to fulfill their legal objectives.

With respect to SSB orders, Principle 5 of the Manila Principles states that the principle of proportionality calls for limitations on both the scope and implementation of the order: "Orders must be limited to specific content violating the law authorizing the order, employ the least restrictive technical means, and be limited in duration and geographic scope."[290] Broad website, service or application blocking would appear to be, by definition, not the least restrictive mean to stop illegal content, since it blocks an entire website or service when only some of its content or uses are illegal.

If a service, application or website is not used exclusively for illegal purposes, the "least restrictive means" test may be fulfilled by narrowing the scope of blocking orders—that is, ordering only specific URLs containing illegal material to be blocked, rather than blocking the entire website or service. Another potential step to comply with the "least restrictive means" is for the court to ask the webmaster or the speaker/owner of the content to take the offending content down prior to issuing the blocking order against an access provider.

In general, authorities responding to unlawful content should develop a sequence of possible interventions from the least intrusive to the most intrusive. SSB, which would be considered the most intrusive measure, should be considered only if the less intrusive remedies do not adequately protect the conflicting right. When considering more restrictive measures, the court or authority should always reassess the balance of the rights at stake and the proportionality of the measure to be adopted; in other words, it should not restrict access to content before trying less-restrictive measures if there is no grave and imminent danger posed by the content at issue.

D. Thematic Findings and Trends

Our thematic findings are based on the human rights documents summarized and the national developments captured in the Appendix to the Report. The highlights of these national developments in the OAS countries are as follows:

- While the existing communication and intermediary liability laws in Argentina appear to favor freedom of expression and oppose SSB, there have been several attempts to pass laws that would allow ISP level SSB.[291] This trend in Argentina is also manifested in SSB orders issued by courts in IP law cases against websites such as the Pirate Bay.[292]

---

the General Comment 34, Freedom of Opinion and Expression, also issued by the Human Rights Committee.)

[290] Principle 5, Manila Principles.

[291] Ley Nacional Contra La Discriminación https://www.vialibre.org.ar/wp-content/uploads/2015/07/DICTAMEN-ACTOS-DISCRIMINATORIOS-Final.pdf [https://perma.cc/F4DJ-L9CC]; For more information see (in Spanish): https://medium.com/@javierpallero/responsabilidad-de-intermediarios-de-internet-en-argentina-4ba3bd51fb67 [https://perma.cc/ABX7-5P7D]

[292] Argentina First in Latin American to Block Pirate Bay, Panama Post (Jul. 1, 2014), https://panampost.com/panam-

- Brazil has seen a number of blocking orders, with the mobile application Whatsapp having been blocked more than once, affecting millions of people in Brazil and other countries.[293] WhatsApp was blocked for refusing to comply with a court order demanding release of communications and information (metadata) about users. Many experts believed the block violated the Marco Civil, which does not allow for blocks, but only the suspension of a determined set of activities for companies that violate users' privacy, data protection, and secrecy of communication rights. Some blocks were also issued based on other more general laws such as the Brazilian Electoral Law.[294]
- In Canada, the provincial government of Quebec passed Bill 74, which allowed DNS blocking through ISPs for gambling websites.[295] However, the proposed law has seen opposition and has been challenged before the Superior Court.[296]
- In Colombia, the law against child pornography, Law 679 of 2001,[297]requires ISPs to engage in blocking mechanisms. However, other laws may be used against intermediaries that have an indirect effect of restricting free expression. For example, the Ministry of Transportation filed a lawsuit to obtain a site-blocking order against Uber for violating local transportation laws.[298]
- There is a similar trend in Cuba, which does not have a direct law for SSB. Resolution No.179/2008 is a general broadly worded law that allows restriction of sites and applications that are contrary to social interests, ethics and morals and/or against the security of the state. This broadly worded law has been used to block websites like Yahoo.
- The USA considered but ultimately rejected SOPA, legislation which would have mandated site-blocking based on copyright infringement. Although SOPA failed, there have been some instances of SSB, most prominently through DNS seizures.[299]

---

staff/2014/07/01/argentina-first-in-latin-america-to-block-the-pirate-bay/ [https://perma.cc/EWD2-2JK3].

[293] The blocking of the WhatsApp application affected directly 100 million of users *(*Alberto Alerigi Jr and Guillermo Parra-Bernal, *Brazil judge orders WhatsApp blocked, affecting 100 million users*, Reuters: Technology, (May 3, 2016), http://www.reuters.com/article/us-facebook-brazil-whatsapp-idUSKCN0XT1KB [https://perma.cc/J7ND-35UU].

[294] For further information on this case, including the original decision and the appellate court decision (in English and Portuguese), see: http://bloqueios.info/en/casos/block-for-non-compliance-with-judicial-requests-for-content-removal/ [https://perma.cc/ZA4T-6ZH2].

[295] *Quebec to require ISPs to block websites*, Internet Society, (July 13, 2016) https://www.internetsociety.org/blog/north-america-bureau/2016/07/quebec-require-isps-block-websites [https://perma.cc/X3PN-R6VE]; Meghan Sali, *Québec is gambling with Internet censorship: what is Bill 74 and how can we kill it?*, OPEN Media, (July 7, 2016) https://openmedia.org/en/quebec-gambling-internet-censorship-what-bill-74-and-how-can-we-kill-it [https://perma.cc/2D9Q-E8D6].

[296] Giuseppe Valiante, Quebec Can't Block Access To Websites Without Permission, (July, 9, 2016) http://www.huffingtonpost.ca/2016/09/02/quebec-websites-crtc_n_11841388.html [https://perma.cc/XQC3-XTFQ]; Steven Stradbrooke, Telecom regulator suspends action on Quebec's Bill 74, (Dec.10, 2016), https://calvinayre.com/2016/12/10/business/canada-regulator-suspends-action-quebec-bill-74/ [https://perma.cc/2J56-6S3G]

[297] LEY 679 DE 2001, http://www.secretariasenado.gov.co/senado/basedoc/ley_0679_2001.html [https://perma.cc/SE5T-MATZ].

[298] For further information, See "Para bloquear a Uber se tendría que bloquear también a Google" , El Espectador, (Mar 24, 2017) http://www.elespectador.com/economia/tribunal-de-cundinamarca-admitio-demanda-contra-uber-interpuesta-por-mintransporte-articulo-684526 [https://perma.cc/W44N-8RVD].

[299] Department of Justice, *Department of Justice Seizes More Than $896,000 in Proceeds from the Online Sale of Counterfeit Sports Apparel*, (April 10, 2012)

Drawing on these and other developments reviewed, we have identified the following trends and thematic findings:

1. Blocks Are Not Based on Clear Legislative Provisions

In most of the cases we reviewed, countries did not have specific legislation concerning the blocking of content, websites or applications at the ISP level. This means that the blocking orders observed in the region are usually based on vaguely worded, ambiguous, or non-specific legal provisions. As explained in further detail in Appendix A, at least in Brazil and Argentina, courts' general powers to order precautionary measures were used to issue blocking injunctions against applications[300] or websites.[301]

We observed that the most common exception to this was regarding protection of children against pornography, sexual abuse, or to protect minors against access to offensive or undesired content. However, even in these cases, the existing legal provisions are sometimes vague and do not necessarily provide all the essential safeguards identified in OAS and other human rights documents to protect the right to freedom of expression.[302]

2. Network Neutrality Provisions May Represent an Important Instrument to Avoid Blocks or To Ensure Courts Are Involved In Blocking Requests

In some countries, Network Neutrality provisions proved to be an important safeguard against excessive SSB. This argument seems particularly important with respect to private blocking, but, in some cases, has been used for blocking by agencies or courts as well. As network neutrality legislation makes it illegal for ISPs to throttle or to block content, authorities in some countries have interpreted these provisions as forbidding the blockage of apps upon request of administrative authorities. This is precisely the case currently under discussion in Colombia, where the Transport authority is trying to block the Uber application, while the Ministry of Communications says that would violate network neutrality provisions.[303] Network neutrality laws in Colombia have one express and specific exception for blocking, in the case of child pornography.[304] The Uber case was brought to a Court in early 2017 by the Transport authority. Although the app at issue is not generally significant for to freedom of expression, the case illustrates how network neutrality provision may be useful to ensure that an independent court assesses the proportionality and legality of the blocking measure proposed by an administrative authority.

---

https://www.justice.gov/opa/pr/department-justice-seizes-more-896000-proceeds-online-sale-counterfeit-sports-apparel [https://perma.cc/3QQX-GSQW].

[300] Check, for example, the WhatsApp cases in Brazil, explained in Part A.1.b.

[301] Check, for example, the Leakymails case in Argentina, explained in Part A.1.a.

[302] See discussion *infra* Appendix A for Colombia, France, India.

[303] For further information, See "Para bloquear a Uber se tendría que bloquear también a Google" , El Espectador, (Mar 24, 2017): http://www.elespectador.com/economia/para-bloquear-uber-se-tendria-que-bloquear-tambien-google-mintic-articulo-686109 [https://perma.cc/64MZ-NFY2] (in Spanish)

[304] Article 56 of Law 1450 of 2011, the Colombian Network Neutrality law, http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43101#56 [https://perma.cc/R2WY-9H9V].

The use of the network neutrality provisions as an argument against blocking was also identified in experts' analysis in Brazil,[305] notably in the case of the successive WhatsApp blocks by courts in that jurisdiction.

3. In the Region, Legislation and Agreements Between Intermediaries and Government Agencies Have Mandated ISPs to Include Clauses on their Contracts to Allow Blocking and Other Content Removal Measures.

In at least two OAS countries, legislation or agreements have required ISPs and other intermediaries to insert clauses allowing content blocking in their terms of service.

In Colombia, for example, legislation on child pornography mandates ISPs to incorporate in the contracts with their subscribers clauses allowing the blocking of content.[306] In Brazil, an agreement established within the Humaniza Redes initiative (a Ministry of Justice initiative to protect human rights on the internet), mandated the Brazilian Internet Association (ABRANET) to recommend its member insert clauses in their contracts which, while not a mode of SSB, have similarly sweeping effect. The clauses allow the termination of accounts used to disseminate child pornography and contents considered to be discriminatory.[307]

Although both initiatives pursue the protection of human rights and the Brazilian initiative does not address SSB, it is important to monitor this kind of development. As mentioned throughout this report, the international human rights law and documents provide a high substantive and procedural threshold that must be met to restrict the free flow of information through extreme measures such as website, service or application blocking. This threshold includes, among other things, that the decision is issued by a court or other independent authority, that safeguards are in place to avoid over-restriction, and that certain transparency and due process rules are respected. Framing the implementation of restrictions of content and the adoption of grave measures such as blocking at ISP level content as a contractual matter may seriously undermine the existing guarantees to the right of freedom of expression.

Moreover, without a clear mandate on what qualifies as impermissible speech under an ISP's blocking/takedown policies or a country's laws, users are less able to self-regulate and predict what is an unlawful conduct that might lead to restrictions of speech. Regulation by contract might not comply with the first step of the three-step test, that mandates restrictions on speech to

---

[305] For e.g., Marina Riguera, Bloquear o Whatsapp fere o Marco Civil da Internet, (Dec. 16, 2015) http://www.em.com.br/app/noticia/economia/2015/12/16/internas_economia,718061/bloquear-o-whatsapp-e-contra-o-marco-civil-da-internet.shtml [https://perma.cc/G9H8-ZV4R] and WhatsApp fora do ar e a violação da neutralidade de rede, Migelhas (Dec. 18, 2015) http://www.migalhas.com.br/dePeso/16,MI231700,21048-WhatsApp+fora+do+ar+e+a+violacao+da+neutralidade+de+rede [https://perma.cc/2E8E-5ZZU].

[306] Article 10, para 2, of Law 79 of 2001.

[307] The Humaniza Redes initiative can be found at http://www.humanizaredes.gov.br/ [https://perma.cc/D6FQ-D8GU]. (The content of the agreement was not available on the website, was obtained by the authors of this report in response to a FOI request and is now available at http://cyberlaw.stanford.edu/page/wilmap-brazil) [https://perma.cc/CK42-B5A9].

be clearly established (materially and procedurally) by law.

4. Service Blocking Has Been Applied Out Of Its Permissible Scope under Human Rights Law and In a Disproportionate Manner In Order To Achieve Other State Objectives

Ordinarily, blocking should be applied only as a proportionate measure to protect one of the larger interests specified in international human rights documents, such as war propaganda and hate speech inciting violence, direct and public incitement to genocide, and child pornography. Instead, some examples identified by this report reflect orders that restrict human rights by couching themselves within secondary goals. In Brazil, the WhatsApp mobile application was blocked for refusing to grant law enforcement access to the communications and metadata of users under investigation. This example demonstrates that even government-ordered blocks that stem from law or judicial processes can enact blocks that can threaten users' rights.

5. Blocking orders against specific egregious forms of content find some support in international human rights law, but may nonetheless be improper if they lack proper safeguards.

Some egregious content, such as child pornography, has served as legal grounds to justify compulsory blocking with lower scrutiny. In some countries, the law may require ISPs to block specified content on these grounds without a court's adjudication.[308] This approach finds some support in international human rights documents,[309] especially in establishing what kind of content is clearly out of the scope of protection of a freedom of expression right. Restrictions on child pornography easily meet the "compelling objective" requirement under Step 2 of the three-step test.

However, if such blocking obligations were expanded to affect entire sites or services, they might not provide the necessary safeguards for freedom of expression rights, and might not be strictly proportionate or narrowly tailored enough to satisfy Step 3 of the three-step test. The existence of child pornography on a site should not, alone, justify SSB without careful consideration of more well-tailored and proportionate measures. It is important to monitor future developments, as provisions restricting the free flow of information have historically been misused to silence dissent and other kinds of lawful speech. Even restrictions on clearly unlawful content should be undertaken on a case-by-case basis and in accordance with the principles discussed in this report. Legislation and court decisions can be improved to provide adequate safeguards, transparency and due process rights to end-users, intermediaries and speakers.

E. Options and Next Steps

In light of the findings of this report and the international human rights standards to balance freedom of expression with other rights, the OSRFE may consider adopting the following measures:

[308] See discussion *infra* Part VI.1.e.

[309] *See* discussion *supra* Section IV.C.2.b.

a. The OSRFE may consider developing in more detail the "least intrusive measure" identified in many human rights documents, specifically in the context of SSB. The research done indicates that it is possible to imagine a sequence of possible interventions from the least intrusive to the most intrusive be implemented before issuing a targeted block or a block against an entire service or website;
b. In the extreme cases where blocks might be granted (after exhaustion of all other lesser intrusive measures), there is still the need to develop appropriate safeguards related to transparency and due process guarantees to end-users, intermediaries and speakers. The OSRFE may consider asking member states to explain any current legislation allowing SSB in each jurisdiction and if transparency, due process and other safeguards to freedom of expression are incorporated in the existing legislation. The OSRFE may consider promoting new standards of transparency, due process and safeguards to freedom of expression through measures such as providing Internet users with notice and an opportunity to challenge ISP blocks on of websites;
c. Some human rights documents indicate that governments around the world are pressuring intermediaries to incorporate specific clauses and conditions in their terms of services that might allow them to voluntarily restrict speech on their platforms/networks. At least in one case, a reported agreement was not publicly available on the Internet.[310] As this practice might entail SSB, the OSRFE may consider asking member states to provide full transparency on planned or existing agreements of this sort, The OSRFE may consider affirming that this kind of agreement should be subject to the highest standards of active transparency, and that member states should proactively make this information publicly available;
d. The OSRFE may consider asking the member states directly and calling upon OAS countries to actively implement a high standard of active transparency to inform the public about websites and services that have been blocked. Member States that engage by any means in SSB should provide a full and detailed list of the measures adopted,[311] the technical means to implement it, and the legal reasons that justify such severe measures.
e. Some human rights documents affirm that the blocking of entire websites is incompatible with ICCPR Article 19, para 3, while others state that "the adoption of mandatory measures to block and filter specific content is admissible" only in "exceptional cases of clearly illegal content or speech that is not covered by the right to freedom of expression."[312] The OSRFE may provide further detail on what would characterize these "exceptional cases," and may consider advancing an interpretation that clearly limits extreme measures only to "expression that constitutes an offence under international law and can be prosecuted criminally."[313]
f. The OSRFE may consider encouraging intermediaries and governments to engage in

[310] World Intermediary Liability Map: Brazil, *supra* note 307.

[311] This recommendation was previously made by the UN Freedom of Expression Rapporteur. *See* A/HRC/17/27 at para 70.

[312] IACHR OSRFE (2013), at para 85.

[313] Report of the Special Rapporteur on the Promotion and Protection of the Right to freedom of Opinion and Expression (August 2011) (Frank La Rue) Document No.: A/66/290. Available at: http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf [https://perma.cc/RQ9U-BH46] at para 18.

multistakeholder discussions to review any exceptional blocking measures that are adopted, assess their legality and compliance with international human rights standards, and to restrict to the minimum the use of this severe measure;

g. In some cases, courts have ordered SSB without meeting the high threshold of international human rights law, such as the three-step test. The OSRFE may consider encouraging member states to promote trainings and capacity building activities with judges, prosecutors and other members of the judiciary.
h. The OSRFE may consider inviting countries in the Inter-American system to study the effectiveness of the restrictions their governments have previously implemented.

F. Conclusion

This Part of the report explores the tensions between the blocking of entire websites and services, and the right to information and freedom of expression. It also explores how the international human rights documents and the OAS framework for freedom of expression treat orders that block websites or services and how it may limit such blocks. It concludes that the OAS framework, and international human rights law generally, demand that a high threshold be met to allow the implementation of blocking measures at the ISP level. Measures against entire websites or services are deemed so severe that they should not only be subjected to this high threshold, but applied only in very exceptional situations, such as when all content on the site is clearly out of scope of the protection of freedom of expression in international human rights law and no less restrictive measure is possible.

The report identified instances where SSB orders were issued without due consideration for the international human rights standards, and noted that legislation and court decisions frequently lack safeguards to adequately protect freedom of expression. Significant effort is still required to ensure that blocking orders are issued only in exceptional situations. Pertinently, even when dealing with the most egregious and extreme cases, countries need to further develop their laws to ensure proportionality, to guarantee due process rights and transparency to all parties affected directly or generally.

PART V: CONCLUSION

This Report examined two types of restrictions that have been imposed to the free flow of information and that target internet intermediaries: the so-called "right to be forgotten" and the site and service blocking implemented at the Internet Service Providers level. By analyzing more than 25 human rights documents, including conventions, reports from different international bodies, and documents from civil society groups, the research explored whether and how the international and Organization of American States ('OAS') human rights frameworks can be reconciled with these emerging trends.

One of the primary goals of the research was to identify laws, policies and enforcement practices that pose a threat to freedom of expression on the Internet, including by incentivizing content removal/self-censorship of lawful content by intermediaries. The review of human rights documents yielded valuable guidance on intermediary liability laws and the potential threats they can create for rights of free expression and information access. In particular, the civil-society-drafted Manila Principles provide concrete guidance for enforcement of intermediary liability laws in a manner consistent with international human rights commitments. The Report also aimed to analyze safeguards and remedies against violation of these rights, including procedural protections that can prevent lawful content from being suppressed through intermediaries' "notice and takedown" practices.

This Report discusses and analyses one of the primary sources of human rights in the OAS countries, the American Convention on Human Rights ('ACHR'). The ACHR provides particularly broad protection to freedom of expression rights, and establishes a three-step test for restrictions to the free flow of information. The three-step test demands that any limitation to the freedom of expression must: (i) have been defined in a precise and clear manner by law, in the formal and material sense; (ii) serve compelling objectives authorized by the Convention, and; (iii) be necessary in a democratic society to serve the compelling objectives pursued, strictly proportionate to the objective pursued, and appropriate to serve said compelling objective. Consistent with this test, many human rights documents and reports point out to the necessity of adequate safeguards that ensure due process rights and the right of recourse to all parties affected by Internet content removals, as well as broad transparency to the parties and the general public. Because Internet intermediaries are placed in the position of 'gatekeepers' to the Internet and may have incentive to silence even lawful speech to avoid the risk of liability, human rights documents and reports have also emphasized the importance of independent judicial determination about whether content is unlawful before intermediaries can be required to remove or erase it.

Many of the points emphasized in the OAS human rights guidance on intermediary liability and free expression rights are in tension with the so-called right to be forgotten ('RTBF') as framed by the European Court of Justice ('CJEU') in the *Google Spain* case. Although an increasing number of requests to be "forgotten" are being made in the member states of OAS, and some states have data protection legislation modeled on that applied by the European court in *Google Spain*, the development of the region's jurisprudence is inconsistent. In some cases, courts have permitted claims to be brought not only against search engines, but also media companies. At least one country (Mexico) has upheld stronger procedural protections than are recognized in the European

jurisprudence, rejecting an RTBF order on due process and free expression grounds because the affected publisher was not involved in the proceedings against the search engine. And another (Colombia) has rejected the imposition of RTBF liability on a search engine, saying that this burden should instead fall on the original publisher.

Substantively, the idea of a RTBF has been heavily criticized in the region, given the recent history of authoritarian regimes in some countries and serious concerns about citizens' right to know or to remember. Procedurally, the vagueness of the concept raises concerns related to the first step of the three-step test, and the designation of private Internet companies as adjudicators of RTBF requests conflicts with the procedural safeguards urged in many regional human rights documents.

In terms of site and service blocking ('SSB'), the report identified that many human rights documents strongly condemn measures that suspend access to entire sites or services, and affirm that their implementation should be exceptional and subjected to the highest scrutiny. Nevertheless, around the world, orders compelling ISPs to block websites or applications are increasingly common. In many cases, such orders seem hardly compatible with article 19, paragraph 3 of the International Covenant on Civil and Political Rights ('ICCPR') and the protective framework established by Article 13 of the ACHR. The exceptional situations identified by the reviewed documents involve content outside the protection of freedom of expression rights in international law, such as child pornography and war propaganda. Even in these cases, the sources indicate, content restriction measures must be tailored to target only the unlawful content, for example by blocking individual unlawful pages rather than entire websites. Such measures additionally should be subjected to the three-step test, and be accompanied by broad procedural safeguards to enable the right to recourse for all interested parties. Protecting both free expression and due process rights of Internet users requires transparent disclosure of information to the affected parties, in particular the operators and users of blocked websites, applications, or services.

Implementing blocking orders against entire websites or services typically conflicts with the mandate to use the least restrictive measure when limiting the exercise of freedom of expression. Such broad blocks may not be justifiable unless member states attempt less restrictive alternatives before considering issuing blocking orders. At least in two countries, however, SSB orders were issued, disrupting the right to communicate freely for thousands or millions of users, as a means to ensure compliance by intermediaries with local domestic laws.

Finally, it is important to emphasize that the existence of network neutrality rules prove to be an important safeguard or argument against disproportionate blocks in some countries. In some cases, the existence of this kind of regulation forced the issue to be brought before a court, as in the recent case of Uber, pending before a court in Colombia.

In the light of foregoing, this Report suggests next steps to the Office of the Special Rapporteur for Freedom of Expression ('OSRFE') of OAS to enhance the protection of freedom of expression on the internet. Among other things, the report encourages the capacity building of data protection authorities, judges, and other government actors in the existing international human rights rules and norms relating to intermediary liability and free expression. This includes both

important procedural considerations to limit excessive content removal or suppression by Internet intermediaries, as well as broader and proactive transparency by member states relating to these types of content restrictions.

While, it is certainly an ambitious task to accomplish, the preservation of the freedom of expression is imperative to preserve the democracies that countries of the region have built over many years.

Appendix A: Analysis by regions

This Annex describes how different national authorities have dealt with legal questions discussed in Part II and III of the Report. This section is by no means an exhaustive illustration of RTBF and SSB around the world or within individual countries, but highlights the legal treatment of both or one of the issues in select countries, chosen on the basis of their reported decisions on the subject and the availability of information online. As mentioned, this selection should not be read as a complete survey of the existing case law in the regions or within the countries listed, as the degree of availability of judicial and administrative decisions is diverse among the countries of the region.

1. States in the OAS region

Many countries from Latin America share a common history of authoritarian regimes and exist currently under varying degrees of institutional capacity. In this context, it is not a surprise that the OAS region historically has given a stronger protection to freedom of expression as a tool "to strengthen the operation of deliberative and pluralistic democratic systems through the protection and promotion of the free circulation of information, ideas and expressions of all kinds."[314] At the same time, important differences in national law affect legal developments in the areas reviewed. For example, several countries in Latin America have data protection laws modeled after the European Data Protection Directive, like Argentina, Uruguay, Perú, and Colombia. It is important to consider the legal context of individual states, especially in perspective with their obligation under the Inter-American human rights system.

a) Argentina

Argentina's data protection laws are reflected in its Constitution, the Personal Data Protection Act (Law 25.326, from 2000)[315] and its Regulation (Decree No. 1558, from 2001)[316]. Article 43 of Argentina's Constitution, like many other Constitutions in Latin America, contains a provision regarding habeas data. Argentina's habeas data provision has been described as the "most complete" in Latin America,[317] as it elevates the right of individuals to correct and delete information held about them by both public and private entities: "In case of falsehood of information or its use for discriminatory purposes, a person will be able to demand the deletion, correction, confidentiality or update of the data contained in [public and private] records."[318] Argentina's data protection regime has obtained "adequacy" status for data transfers from the EU,[319] a recognition of its degree of compliance with the European standard. A draft bill for a new

[314] IACHR's OSRFE, (2010), *supra* note 3 at p. 3.

[315] The law can be found at http://www.oas.org/juridico/PDFs/arg_ley25326.pdf [https://perma.cc/WA5W-R454].

[316] The decree can be found at http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/norma.htm [https://perma.cc/K5UU-E47P].

[317] Edward L. Carter, *Argentina's Right to be Forgotten*, 27 Emory International Law Review 23, 33 (2013).

[318] Article 43.3, Argentine Constitution.

[319] Article 29 Data Protection Working Party, Opinion 4/2002 on the level of protection of personal data in Argentina (Adopted 3 October 2002).

data protection act was posted online for comments in February 2017. The proposed changes to the Argentine data protection framework reflect changes in Europe's General Data Protection Regulation ('GDPR').[320]

Whether intermediaries must de-list their search results in response to complaints by individuals has been litigated heavily in Argentina.[321] The most important case, however, did not involve a data protection claim, but the balancing of the conflicting interests of privacy and honor against freedom of expression. Argentina's Supreme Court in 2014 provided guidance on this balance in *Belen Rodriguez* case[322] wherein the court found that intermediaries cannot be strictly liable for content which might impact on the rights of privacy or reputation of others, and except in cases of manifestly unlawful content, should not be obliged to de-list information without judicial or administrative proceeding. In 2016, lawmakers considered passing a bill[323] that criminalized posting "discriminatory" comments online and required online platforms to monitor and take down comments based on vague and ambiguous criteria.[324] Such obligations would be inconsistent with both human rights guidance and the Argentine Supreme Court's Belen Rodriguez ruling, discussed above.

With respect to SSB, the Argentina's current telecommunications and intermediary liability rules appear to respect freedom of expression but some proposed legislation has raised concerns. In 2016, a bill that would allow officials to order ISPs to block apps and websites without first obtaining a court order was introduced. Lawmakers have suspended voting on the bill but it appears that the underlying goals and the bill have not been entirely abandoned.[325]

In the City of Buenos Aires, a Bill was proposed in 2016 to modify a Criminal Procedures legislation in order to implement total or partial site-blocking as a measure to prevent illicit activities that take place or produce effects in the City. The bill was heavily criticized for formal and material problems by civil society groups.[326]

---

[320] *See* Pablo A. Palazzi, *New Draft of argentine Data Protection Law Open for Comment,* (Feb.8, 2017) https://iapp.org/news/a/new-draft-of-argentine-data-protection-law-open-for-comment/ [https://perma.cc/VLL8-NX3T].

[321] *See* Edward L. Carter, Argentina's Right to be Forgotten 27 Emory International Law Review 23 (2013); *Emerging Patterns in Internet Freedom of Expression: Comparative Research Findings in America and Abroad*, Latin American Regional Meeting on Freedom of Expression and the Internet Buenos Aires Argentina (October 19, 2010) http://www.palermo.edu/cele/libertad-de-expresion-en-Internet.pdf [https://perma.cc/W27G-DLGZ]

[322] Corte Suprema de Argentina, "Rodríguez M. Belen c/Google y Otro s/ daños y perjuicios," Judgment R.522.XLIX, 10/28/14.

[323] LEY NACIONAL CONTRA LA DISCRIMINACIÓN https://www.vialibre.org.ar/wp-content/uploads/2015/07/DICTAMEN-ACTOS-DISCRIMINATORIOS-Final.pdf [https://perma.cc/F4DJ-L9CC].

[324] David Bogado, *No to Internet Censorship in Argentina*, Electronic Frontier Foundation (Aug. 11, 2015), https://www.eff.org/deeplinks/2015/08/no-internet-censorship-argentina.

[325] Javier Pallero, *App Blocking in Argentina: a bad idea that must be dropped permanently,* ACCESS NOW, (Sept. 7, 2016) https://www.accessnow.org/app-blocking-argentina-bad-idea-must-dropped-permanently/ [https://perma.cc/FG9D-BBB2].

[326] *See also* (in Spanish) *Un proyecto de ley que pone en riesgo la libertad de expresión en Internet,* (Sug.29, 2016) https://adcdigital.org.ar/2016/08/29/proyecto-ley-pone-riesgo-la-libertad-expresion-internet/ [https://perma.cc/9XBM-ZDJZ].

On the national level, another Bill (D-5771-2016) addresses the liability of internet intermediaries and provides definitions of clearly illegal content (that must be eliminated, blocked, de-indexed, or removed after a request) and illegal content (that must be eliminated, blocked, de-indexed, or removed after a court order). If approved, the bill would allow any person that "feels affected" by content on the Internet to file a lawsuit seeking the elimination, blocking, de-indexation or removal of content. The bill was criticized by public interest experts on Internet regulation.[327]

In the past few years, there have been several site-blocking incidents that received attention in the media. In 2014, a court ordered ISPs to block access to The Pirate Bay, a file sharing site, on the grounds that the website content was violating copyright laws.[328] In August 2011, the National Criminal Court ordered[329], based on general powers to issue preliminary injunctions established in the Argentine Penal Code and Criminal Procedures Code, all ISPs to block the site LeakyMails.com and LeakyMails.blogspot.com. LeakyMails was a website that obtained and published documents exposing corruption in Argentina.[330] The government's request to "block an IP address identified as the LeakyMails Web site … reportedly affected thousands of Internet users."[331] In response, "some service providers in Argentina [blocked] access to the IP address 216.239.32.2, which [was] linked to more than one million blogs hosted on Google's Blogger service."[332] Even if one ignores whether the content in this case was lawful, the incident exposes the lack of proportionality in the implementation of a blocking order, making the absence of a method for assessment of adequacy and proportionality, such as the three-step test, evident.

Other reported blocks in Argentina before 2013 can be found in the CELE's report Internet en Argentina: ¿cómo estamos hoy?[333]

---

[327] For more information see (in Spanish) Javier Pallero, *Responsabilidad de intermediarios de Internet en Argentina*, (Sept.13, 2016). https://medium.com/@javierpallero/responsabilidad-de-intermediarios-de-internet-en-argentina-4ba3bd51fb67 [https://perma.cc/ABX7-5P7D].

[328] *Argentina First in Latin American to Block Pirate Bay*, Panama Post (Jul. 1, 2014), https://panampost.com/panam-staff/2014/07/01/argentina-first-in-latin-america-to-block-the-pirate-bay/ [https://perma.cc/EWD2-2JK3].

[329] Juzgado Nacional en lo Criminal y Correcional Federal Nro. 9, Nro. 9177/11 "N.N. s/relevacion de secretos politicos y militares," (Aug. 4, 2011), https://advox.globalvoices.org/wp-content/uploads/2011/08/ADJ-0.991681001313004665.pdf [https://perma.cc/F2TS-29HB].

[330] Renata Avila, *Argentina: Judge orders all ISPs to block the sites LeakyMails.com and Leakymails.blogspot.com* (Aug. 11, 2011), https://advox.globalvoices.org/2011/08/11/argentina-the-national-communications-commission-ordered-all-isps-to-block-the-sites-leakymails-com-and-leakymails-blogspot-com/ [https://perma.cc/RDM4-XYRK].

[331] U.S. Dep't of State, Country Reports on Human Rights Practices, Argentina. Page 11 (2011), https://www.state.gov/documents/organization/186697.pdf [https://perma.cc/8S9R-R95J]. And (In Spanish).Por un error en el bloqueo a "leakymails," salen de servicio un millón de blogs, Clarín (Aug. 28, 2011) https://www.clarin.com/politica/bloqueo-leakymails-servicio-millon-blogs_0_SJgbu7R2Dmx.html [https://perma.cc/3Z7D-PSN3].

[332] Jillian C. York, *Argentinian ISPs Use Bazooka To Kill Fly* (Aug. 19, 2011), https://www.eff.org/deeplinks/2011/08/argentina-isps-ip-overblocking [https://perma.cc/RV5T-28Y4].

[333] CELE and UP, *Internet en Argentina: ¿cómo estamos hoy? Mapeo de la situación en materia de acceso, regulación, y derechos humanos*, http://www.palermo.edu/cele/pdf/investigaciones/Mapping-ARG-CELE.pdf [https://perma.cc/SYZ5-PUXH] Pages 7-8 (in Spanish)

b) Brazil

Brazil does not have a data protection Law on the books, although it has opened a consultation to seek input towards passing one and now it is in the works in Congress.[334] Nevertheless, other laws impact the ways in which Brazilians use and access information online and interact with intermediaries. Most notably, the Brazilian Civil Rights Framework for the Internet ("Marco Civil") from 2014 is applicable to every kind of Internet activity. Marco Civil has a chapter on Fundamental Rights that recognizes personal data protection and gives individuals the right to be informed and requires data controllers to obtain consent from users before processing their data.

Article 7 of Marco Civil also gives citizens the right to request the definitive elimination of personal data provided by the user to an Internet company, at the end of the relationship between the parties. Regarding intermediary liability, Marco Civil establishes that in most cases providers of Internet applications can only be deemed liable for content generated by third parties if they do not respect a court order to take it down. In such removals, intermediaries must also, when possible, notify the original publisher of that information to allow her to legally contest and submit a defense in court. Further, when requested by the original publisher, intermediaries should replace the content so removed with an explanatory note about the court proceedings.[335]

Brazilian courts have adjudicated a series of cases against search engines. These cases involved the balancing between personality rights and the right of access to information and were decided in favor of the search engines. In a decision from 2012, Brazil's Superior Court of Justice found Google not liable for making available a set of links and pictures in relation to a television actress because it would compromise access to information.[336] Recently, in November 2016, the same Court decided another case against Google where a person had asked the search engine to remove search results to websites and images associated with her name. In its opinion, the Court categorically affirmed that search engines cannot be compelled to de-list all results for particular search queries.[337]

Given the strong framework provided by the Marco Civil and the lack of a data protection law, Brazil has shown a consistent approach towards cases involving search engines. Their clearly defined rules for intermediary liability seem to have been instrumental in safeguarding the role of

---

[334] Bruno Bioni, Renato Monteiro. *Is Brazil finally walking towards a General Data Protection Law?*, IAPP Privacy Tracker, https://iapp.org/news/a/is-brazil-finally-walking-towards-a-general-data-protection-law/ [https://perma.cc/6SYS-JGCW].

[335] An exceptional case on which a private request is enough instead of a court order is when the content published by the third parties contains images, videos and other materials containing nudity or sexual activities of a private nature, published without the authorization of the participants (a set of cases commonly associated under the Revenge Porn category).

[336] Superior Tribunal de Justiça. Recurso Especial No 1.316.921 - RJ. *Google Brasil Internet LTDA. vs. Maria da Graça Xuxa Meneghel.* June 26, 2012. http://www.internetlab.org.br/wp-content/uploads/2017/02/STJ-REsp-1316921.pdf [https://perma.cc/YS94-9LPR].

[337] Superior Tribunal de Justiça. Recurso Especial No 1.593.873 - SP. *Google Brasil Internet LTDA. vs. SMS*. November 10, 2016. http://www.internetlab.org.br/wp-content/uploads/2017/02/STJ-REsp-1.593.873.pdf [https://perma.cc/2XUE-HHQK].

search engines and differentiating them from the original publisher of the content. However, two things must be emphasized: i) once a data protection law is approved in the country and if a data protection authority is established, the direction of courts might shift; ii) the validity of RTBF claims based on privacy rights or on the protection to reputation are not yet resolved in the Brazilian jurisprudence, as demonstrated by the cases reaching superior courts in the country, briefly described below.

The Superior Tribunal de Justiça (STJ) has decided some cases, not based on data protection, but that are related to the RTBF debate. In the first case, decided in May 2013[338], STJ recognized a "right to be forgotten" based on a privacy claim against Rede Globo, a TV broadcaster in the country. In this case, the plaintiff, who was accused and finally acquitted for participating in a slaughter in front of the Candelária Church, succeeded in obtaining damages from the media company for having his name associated with the episode. The Court decided that it would be possible for the media to tell the story without mentioning the plaintiff's name.

In a second case, the same court decided in 2013 a claim against the same company. In this case, the plaintiffs (relatives of a victim of homicide in 1958 - Aida Curi), affirmed that the broadcasting of information about the crime reopened their wounds, and requested damages based on a RTBF claim. The court decided that there was no abuse and that the media company (TV Globo) was informing about public and historical facts, affirming that the facts of the crime were now in the public domain. The decision was appealed to the Supremo Tribunal Federal, where the case is still pending.[339]

In a third case, decided in September 2016 by STJ, the court recognized a RTBF based on privacy and reputation claims to determine the payment of damages by a newspaper that, in an interview, mentioned the participation of the plaintiff in an attack in an airport in the north of the country. One of the justifications used by the decision is based on the fact that Brazil passed an Amnesty Law in 1979, by which different antagonistic forces would have agreed to promote the social pacification of the country, and that would have entailed the "forgetfulness of the conflicts"[340] of the period.

Finally, in a case decided in November 2016, STJ affirmed that there is no legal ground to demand the de-indexation of content from a search engine based on a RTBF privacy/reputation claim. In this case, the court also asserted that the Civil Marco Civil article 7, X, does not entail to a RTBF. The article establishes the right to request the definitive exclusion of personal data transferred to an Internet application at the end of a contractual relationship. The decision,

---

338 *See* full decision (in Portuguese): https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1239004&tipo=0&nreg=201201449107&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20130910&formato=PDF&salvar=false [https://perma.cc/JRF2-PVEP].

339 *See also* Globo Comunicações e Participações S/A v. Nelson Curi et al., https://globalfreedomofexpression.columbia.edu/cases/globo-comunicacoes-e-participacoes-sa-v-nelson-curi-et-al/ [https://perma.cc/3DWA-C2AT]

340 *See* full decision, (in Portuguese): https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1519492&num_registro=201102359630&data=20161028&formato=PDF [https://perma.cc/F298-3XXD].

therefore, affirms that this right does not extend to the public information available on the internet.

With respect to SSB, Brazilian courts have issued a number of controversial blocking orders over the last several years, specifically in connection with the widely used WhatsApp application. The Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression issued by the United Nations in 2016 deemed such blockings in Brazil (along with six other countries) unlawful.[341] The court orders were based on WhatsApp's refusal to disclose to authorities the content of encrypted communications and the metadata, which WhatsApp is required to store and provide upon court order in the course of an investigation. In all the cases, the blocks were reversed upon appeal. The blocks affected millions of people in Brazil[342] and in other countries and attracted enough attention of policymakers and members of congress to be followed by the proposal of bills in Congress to expressly forbid the blocking of messaging apps. In addition, two lawsuits have been filed to declare the blocks (and the parts of Marco Civil used to justify the blocks) unconstitutional[343].

Although the blocking orders against WhatsApp were the most impactful, other blocking orders have been issued against different websites (such as the website Tudo Sobre Todos, for violation of privacy rights) and services (such as the app Secret, for allegedly ensuring anonymity in the platform).[344]

In 2016, the State Court of São Paulo did not grant a preliminary order to block a website that made information in connection with equity interest in companies available, deeming such information public. The court, however, did not address the legality, proportionality or necessity of the measure.[345]

Beyond Marco Civil, some cases sought SSBs based on claims of violation of the Brazilian Electoral Law (Law no. 9,504/97, that establishes rules for the elections process). Article 57-I establishes that the Electoral Court may order suspension, for twenty-four hours, of access to any information content of websites that fail to comply with the provisions of the Electoral Law, at the request of a candidate, party or coalition. The provision allows this period of suspension to be doubled with each repetition of conduct. An example of such restriction was found in Process no. 141-28.2016.6.24.0019 at the Regional Electoral Court of Santa Catarina, in October 2016. Here, the Court ordered the suspension of Facebook for 24 hours if the company did not remove a page criticizing a candidate. Facebook removed the content indicated by the court as unlawful, and filed

---

[341] A/HRC/32/38, (2016) at 13.

[342] The blocking of the WhatsApp application affected directly 100 million of users *(*Alberto Alerigi Jr and Guillermo Parra-Bernal, *Brazil judge orders WhatsApp blocked, affecting 100 million users*, Reuters: Technology, (May 3, 2016) http://www.reuters.com/article/us-facebook-brazil-whatsapp-idUSKCN0XT1KB [https://perma.cc/RV32-C8E6]).

[343] *See* PAULA PÉCORA DE BARROS, ADPF 403 IN STF: ARE WHATSAPP BLOCKINGS CONSTITUTIONAL? (Nov. 21, 2016) http://bloqueios.info/en/adpf-403-in-stf-are-whatsapp-blockings-constitutional/ [https://perma.cc/Y888-CVVP].

[344] For a comprehensive collection of blocking cases, bills and debates in Brazil, see http://bloqueios.info/en/timeline/ [https://perma.cc/FZ7G-SL8Z].

[345] For further information and analysis of this process (number 2177717-09.2016.8.26.0000), *see*, http://omci.org.br/jurisprudencia/125/divulgacao-de-dados-pessoais-e-bloqueio-a-site/ [https://perma.cc/FJP5-T5EE].

an appeal. Considering the removal, the block was never implemented. When deciding the case, the Tribunal Superior Eleitoral pointed out that the blocking order was a severe measure, and that the suspension "of sites on the Internet should respect the appropriate gradation with the severity of the perpetrated illicit conduct, reserving such penalty for when the felonious intent of not complying with the judicial decision is proven, with transparent imbalance of forces on the electoral dispute."[346]

c) Canada

Canada has two federal privacy laws: the Privacy Act (1985) relates to federal government agencies and departments, and the Personal Information Protection and Electronic Documents Act (2000) ('PIPEDA') applies to the private sector.[347] Canada's data protection regime generally tracks the EU's, and therefore meets the requirements of the EU's adequacy standard.[348]

In 2017, the Federal Court of Canada decided a case regarding the interaction of rights conferred by PIPEDA with public information available on the internet.[349] In that case, a Canadian resident filed suit when the Romanian-based respondent failed to comply with his request to remove information about him that was published on the respondent's website, Globe247h.com. The respondent's website aggregated public documents from Canada's court reporting database. The data aggregated on this website was then indexed by search engines (the content of Canada's legal databases was typically not indexed by search engines).[350] The applicant complained that a tribunal decision relating to an employment dispute appeared as a Google Search result in response to a search of this name. The applicant requested Globe247h.com to remove this information from their website, but the site refused to do so without the payment of a fee. The applicant filed a complaint under PIPEDA, which was investigated by the Canadian Privacy Commissioner, who found that the respondent had failed to comply with PIPEDA. The applicant sought damages, as well as declaratory and injunctive relief from the Federal Court. The Federal Court found that PIPEDA had extra-territorial jurisdiction to apply to the acts of the respondent,[351] and that the respondent had failed to comply with PIPEDA. The Court issued a corrective order requiring the respondent to comply with PIPEDA. The declaratory relief anticipates that the applicant (and others affected by the respondent's conduct) use the Court's Order to support requests to Google (and other search engines) that the search results be de-indexed.[352]

---

[346]For further information on this case, including the original decision and the appellate court decision (in English and Portuguese), *see* Facebook Case II
Non-Compliance with Judicial Requests for Content Removal, (Oct.5, 2016), http://bloqueios.info/en/casos/block-for-non-compliance-with-judicial-requests-for-content-removal/ [https://perma.cc/ZE25-S27R].

[347] Office of the Privacy Commissioner of Canada, Fact Sheet (updated May 2014) https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/ [https://perma.cc/BK2N-GW3V].

[348] *See* Secretary General of the European Commission, The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act (21 November 2006).

[349] A.T. v. Globe24h.com (2017) FC 114.

[350] *Id.* at para 9.

[351] *Id.* at para 51-62.

[352] *Id.* at para 86. The Office of the Privacy Commissioner of Canada submitted that this was the most "practical and

In the SSB context, the provincial government of Quebec passed Bill 74 that allowed the direct DNS blocking through ISPs for gambling websites.[353] However, the proposed law has seen opposition and has been challenged before the Superior Court.[354]

d) Chile

There are two laws from Chile that are important for consideration for internet intermediaries. One is Law No. 20435, which modified in 2010 the Intellectual Property Rights Act. As per this modification, a copyright holder may obtain a court order to oblige intermediaries to remove or block infringing content, but may not trigger removal obligations simply by notifying the intermediary. This law was celebrated on introduction[355] and is unique from other similar regulatory frameworks because it requires adjudication by an independent juridical authority.[356] Chile's Law No. 20,453 is aimed at providing net neutrality and prohibits "blocking, interference, discrimination, throttling, and the restriction of the right of any user to use, send, receive or offer any lawful content, application or service through the Internet, as well as any other type of lawful activity on or use of the web."[357]

Additionally, Chile recognizes as a constitutional guarantee the right to privacy and honor of their citizens in Article 19 N 4 of its Constitution. Since 1999, its data protection law has given data subjects the right to request directly to the data controller the elimination or cancellation of personal data registries whenever there's no legal justification for its treatment or it has expired; and to request the modification of the personal data registered when they are mistaken, inexact, equivocal or incomplete.

In 2014, the Court of Appeals of Santiago decided a constitutional case that could be relevant for RTBF. A citizen brought a claim against Google because the search results associated to her name included a defamatory website that alluded to her having AIDS.[358] The Court ultimately rejected the claim because the original content had disappeared from the original source. However, it did say in one excerpt that the possibility of bringing an action against a search engine for content made available by a third party is a concept that in general has been rejected by Chilean

---

effective way" of mitigating the harm to individuals.

[353] *Quebec to require ISPs to block websites*, Internet Society (2016) *supra* note 295; Meghan Sali, (2016) *supra* note 295.

[354] Giuseppe Valiante, (2016) *supra* note 296; Steven Stradbrooke *supra* note 296.

[355] CDT, Chile's Notice and Takedown System, *supra* note 29. *Chile Leads the way on Intermediary Liability Protections* , Techdirt, (Sept. 11, 2012*)* https://www.techdirt.com/articles/20120911/06282620341/chile-leads-way-intermediary-liability-protections.shtml [https://perma.cc/6UZM-BN7K].

[356] *Human Rights and Internet Intermediary Regulation in Chile*, Global Censorship Chokepoints, https://globalchokepoints.org/human-rights-and-internet-intermediary-regulation-chile.html [https://perma.cc/2ZQX-4XNJ]; CDT, Chile's Notice and Takedown System, *supra note* 29.

[357] CHAPTER IV: FREEDOM OF EXPRESSION AND THE INTERNET, at 479, http://www.oas.org/en/iachr/expression/docs/reports/internet/foe_and_internet_report_2013.pdf [https://perma.cc/2VHX-6N2N].

[358] Court of Appeals of Santiago, Fifth Chamber, Decision on Recurso de Protección No. 45.790-2014.September 25, 2014, https://cldup.com/Fp8gDqNpkC.pdf [https://perma.cc/TWV2-RR7V].

courts and referred to two extra cases from 2013 and 2014 that were decided in that sense.[359] More recently, in 2016 the Supreme Court of Chile debated a case against a newspaper regarding an old news article on a criminal investigation, ordering the original publisher to delete the content from its online archives, ignoring less restrictive alternatives such as the rectification of the original content or the use of robots.txt and/or other technical means to prevent indexation by the search engines without the suppression of content.

e) Colombia

Colombia protects freedom of expression and freedom of the press rights in its Constitution, Article 20[360]. The Constitution also recognizes the right to privacy and personal data protection.[361] It provides no censorship against mass communication media. However, the rights under this article are applicable only to "true and impartial" information. Article 73, furthermore, emphasizes this protection in terms of journalistic activity.

In 2012, Colombia introduced a Data Protection Law (Law 1581), which recognizes the data subject's rights to access, rectification, cancellation and objection to the processing of personal data. In 2015, the Constitutional Court decided the case of *Gloria v. Casa Editorial El Tiempo*, in which a citizen, who was reported on the media to be a part of a human trafficking mafia, asked the newspaper to takedown the content and also to remove it from search engines after the statute of limitations had expired for the crime.[362] The Court said that the real violation of rights wasn't done at the moment of the indexation by the search engine but when the newspaper published the story. Therefore, the Court determined that the newspaper did have a duty to update the news story until its judicial conclusion, but not to delete the content. Additionally, they ordered the newspaper to use technological means (like the robots.txt file and meta tags) to avoid search engines indexing the news story on their website.[363] The Court also acknowledged that search engines could not be held liable for the content published by third parties because this would go against the Network Neutrality Principle of the Internet and that Colombian courts lacked the jurisdiction to order Google Inc., a company based in the United States, to take an action. In direct reference to the solution offered by the CJEU in the *Google Spain* judgment, the Colombian Constitutional Court deemed it an "unnecessary sacrifice of the Network Neutrality principle and, with it, of the freedom of information and expression."

The Colombian Court reached a decision very different from the CJEU in a range of

[359] 11 de noviembre de 2013, rol 80.700-2013; y del 15 de enero de 2014, rol 139.347 – 2013.

[360] Article 20 and 73, the Constitution of Colombia https://www.constituteproject.org/constitution/Colombia_2005.pdf [https://perma.cc/23Z3-R6U9].

[361] Article 15, Colombian Constitution.

[362] Constitutional Court of Colombia, SENTENCIA Nº T-277, Gloria v. Casa Editorial El Tiempo. May 12, 2015. https://karisma.org.co/wp-content/uploads/2015/07/TUTELA-EL-TIEMPO.pdf [https://perma.cc/KF4Q-VW6S]. .

[363] The Robot Exclusion Standard or "Robots.txt" is a technical standard that any website can use as a tool tell search engines to ignore certain sections or URLs of their website in their search result. As a consequence of the implementation of this tool, a website will be effectively unreachable through a search engine. Koster, Martinj. "About /robots.txt" http://www.robotstxt.org/robotstxt.html [https://perma.cc/8X2H-JQKZ].

respects. Despite trying to more equally balance rights than the CJEU in the *Google Spain* judgment, it perhaps inadvertently ordered broader delisting than the CJEU did. By ordering the use of a mechanism like "robots.txt", it ensured that the links would disappear for all search queries on Google -- not merely queries searching for the plaintiff by name.

The law against child pornography, Law 679 of 2001,[364] requires ISPs to engage in blocking mechanisms.[365] The method and standard of this blocking, however, are not stated within the law but are subject to annual review by a specific commission. The law also does not limit the blocking mechanism to a specific URL or content. The law's general language could lead ISPs to block entire sites. Article 4 of the law 679/2001 establishes a commission that can propose technical measures to block and filter content that may be improper for consumption by minors. Further, Article 8 of the law mandates that ISPs provide technical measures that allow users to protect themselves and their children from offensive or undesired content.

The regulation (Decree 1524 of 2002) that details the implementation of this law, issued by the Colombian Ministry of Information and Communications Technologies, establishes technical and administrative measures to protect minors on the Internet. The decree forbids providers and servers to provide access to websites that distribute child pornography, and mandate ISPs to implement technical measures to prevent access to websites containing child pornographic material. ISPs that do not comply with the decree may be subject to fines amounting up to 100 times the local minimum wage.

In a recent case against Uber, the transport authority attempted to get a service blocking order against the Uber mobile application.[366] The request alleged that Uber's service of transport does not comply with local transportation law. The Ministry of ICTs stated that, in respect to the network neutrality legislation in Colombia, the Ministry was not entitled to suspend any kind of application, but only to verify if orders issued by the competent authorities were being complied with by ISPs.[367]

f) Cuba

According to Freedom House, "Cuban law places strict limits on free speech and outlaws independent media." A number of websites are regulated/blocked in Cuba, but it still does not "have the same level of technically sophisticated blocking that characterizes other highly restrictive internet environments", i.e. while the government has imposed blocks, Cubans are able

[364] Ley 0679, *supra* note 297.

[365] *Freedom on the Net 2016*, Colombia at 7 ("According to the ICT Ministry, the only content that is subject to blocking measures is child pornography, which is illegal under international law…")

[366] For further information, See "Para bloquear a Uber se tendría que bloquear también a Google" , El Espectador, (Mar 24, 2017): http://www.elespectador.com/economia/para-bloquear-uber-se-tendria-que-bloquear-tambien-google-mintic-articulo-686109 [https://perma.cc/64MZ-NFY2] (in Spanish)

[367] *Ministerio TIC no bloquea aplicaciones sin orden legal, judicial o administrative*, MINTIC, (July 18, 2016) http://www.mintic.gov.co/portal/604/w3-article-11221.html [https://perma.cc/WN5E-NS3S].

to circumvent these measures.[368] Site blocking can be imposed relatively easily without judicial oversight given the government monopoly in the provision of Internet access. The law Resolution No.179/2008[369] allows Empresa de Telecomunicaciones de Cuba SA (ETECSA), a telecommunication agency, to "take the necessary steps to prevent access to sites whose contents are contrary to social interests, ethics and morals, as well as the use of applications that affect the integrity or security of the state."[370] This law has been used to block local independent news websites, activist and dissident organization websites, and such major portals as Yahoo.[371] In our research, we found nearly no mention of the existence of a RTBF or similar right.

g) México

The Mexican Constitution recognizes the fundamental right to the protection of personal data.[372] Likewise, the Federal Personal Data Law grants individuals the rights to access, rectification, cancellation and objection to the processing of personal data. This law is supervised by the National Institute for Transparency, Information Access and Personal Data Protection held by Individuals ("INAI"), an autonomous administrative agency.[373]

In 2015, INAI initiated proceedings against Google Mexico for denying a businessman the exercise of his rights to cancel and object to the processing his personal data in the search engine results.[374] According to his original request, the businessman wanted to take down a reference to his possible involvement in a corruption scandal as reported in a news piece by *Fortuna* Magazine in 2007. Deciding as the Data Protection Agency, the INAI concluded that Google was indeed a data controller under Mexico's data protection law and legally obliged to act upon the requests of data subjects. Therefore, the company had breached that obligation when denying the claimant's request to cancel and object to the treatment of his personal data.[375] That administrative decision was contested in Court by *Fortuna* Magazine, the original publisher of the information de-listed,

---

[368] Freedom House, Freedom on Net 2015, Cuba, https://freedomhouse.org/report/freedom-net/2015/cuba [https://perma.cc/TYV9-2VY3].

[369] For more information, see Law 179/2008 Article 19, J (in Spanish): http://www.mincom.gob.cu/sites/default/files/marcoregulatorio/R%20179-%2008%20Reglam%20Proveedores%20Serv%20Acceso%20Internet%20al%20Publico.pdf [https://perma.cc/5HTB-DN4B].

[370] *Freedom on Net 2015*, Cuba.

[371] *Id.*

[372] Article 16, Constitution of the United States of Mexico.

[373] Thompson & Knight: Attorneys & Law, Mexican Data Protection Law, (Apr. 26, 2016), http://www.tklaw.com/files/Publication/4a60406f-524f-4312-b527-500b6d82c38c/Presentation/PublicationAttachment/493721a4-f671-425e-81c5-613d8eb79f00/TKClientAlert_MexicoDataProtection.pdf

[374] Red en Defensa de los Derechos Digitales. ¡Ganamos! Tribunal anula resolución del INAI sobre el falso «derecho al olvido». August 24, 2016. URL: https://r3d.mx/2016/08/24/amparo-inai-derecho-olvido/ [https://perma.cc/8KGA-XB57].

[375] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Docket No. PPD.0094/14. Against Google México, S. de R.L. de C.V. January 26, 2015. p. 20. http://inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf [https://perma.cc/F6X7-74PL]

and was initially confirmed at the first instance. However, in August 2016, the Court of Appeals for the First Region in Mexico determined that the right of audience of the publisher was violated by the administrative procedure under controversy.[376] In their decision, the Court considered that the de-listing order given by the Data Protection Agency limited the right to impart information of the magazine publishers and that they should have participated as an interested third party in the administrative proceedings. As a result, the Court declared the administrative decision void and remanded the case for rehearing. In this case the final decision was more procedural than substantial. The Court considered, and weighed against the Constitution and the American Convention, whether a procedure to limit the reach of information could take place without the participation of the original publisher. The regular data protection claim as applied by the INAI wasn't designed to consider the interests of third parties, like the original publisher.

h) Perú

The Peruvian Constitution recognizes that every citizen has a right to privacy and data protection. Since 2011, the right to data protection has been recognized in the data protection law, which grants individuals the rights of access, rectification, cancellation and objection to the processing of personal data. The data protection authority for the country is the Authority for the Protection of Personal Data ("Peru's DPA"), an administrative office within the Ministry of Justice and Human Rights, who has been adjudicating cases since 2013.

In 2016, Peru's DPA decided a case against Google where a former public servant, who had been previously detained by the police for possessing child pornography, wanted to remove any reference to that episode from the search results associated with his name, as they appeared in newspapers, blogs and forums accessible through Google search results.[377] Peru's DPA considered the search engine as a data controller under the Peruvian data protection Law. As such, it ordered Google to block not merely specific identified URLs but *any* search result related to the incident that may appear under the name of the claimant. Later, under administrative appeal, Peru's DPA confirmed his decision and detailed a list of 16 links that were the only ones subject to de-indexing.

The Peruvian case is similar to the Mexican case because both involved the Data Protection Agencies. However, in the Peruvian case the initial order to de-list was much more broad and undefined, effectively requiring Google to proactively monitor and police user expression, in violation of strong prohibitions on such measures by human rights sources. This monitoring obligation was the only aspect of its decision that Peru's DPA corrected under administrative appeal. Again, no extra guidance was given about how this new breed of data controllers (search engines) should proceed under the Peruvian data protection law. This degree of confusion about what is possible under Peru's data protection laws lead recently to a man, who was investigated for narcotics trafficking, convincing a judge to issue a precautionary measure ordering Google and

---

[376] Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región, http://sise.cjf.gob.mx/SVP/word1.aspx?arch=1100/110000001885932400001001.docx_0&sec=_Mercedes__Santos_Gonz%C3%A1lez&svp=1 [https://perma.cc/N8LW-9ZBZ].

[377] Dirección General de Protección de Datos Personales. Directorial Resolution No. 026-2016-JUS. March 11, 2016. http://www.hiperderecho.org/wp-content/uploads/2016/06/datos_personales_google_olvido_2.pdf [https://perma.cc/B6DR-65XS]

every major news outlet of Peru to de-list search results and news with his name in connection with "any false report." The decision was later reversed and the process is still going.[378]

i) USA

Based on the fact that the USA does not have data protection laws on the European model, and because of the country's strong free expression jurisprudence under the First Amendment, RTBF is widely seen as inconsistent with that country's laws. That said, some narrow legal provisions for suppression of truthful personal information do exist,[379] and privacy advocates and scholars have advanced arguments in support of broader rights to be forgotten.[380]

The US Congress famously rejected site blocking mandates in the much-criticized SOPA legislative proposal. Nonetheless, site blocking has since occurred in the United States, most prominently through the mechanism of DNS seizures. For example, in 2010 the Department of Homeland Security initiated operation 'In Our Sites' to "combat online piracy and the proliferation of counterfeit goods on the internet," according to the ACLU.[381] As of 2012, the Department of Justice noted seizure of at least 758 domain names.[382]

2. Countries Outside of the OAS Region

a) China

For certain online violations of privacy one can sue under the provisions, principles, and interpretation of General Principles of Civil Law, 1986; Standing Committee of the National People's Congress Decisions and the PRC Supreme People's Court.[383] However, it is unclear from these laws if ISPs or Search Engines can be sued. Further, China's Tort Liability Law protects privacy and interests of a civil nature but it does not extend to RTBF or personal data specifically.[384] However, Articles 36 and 15 of the Tort Liability Law extend to online torts where

---

[378] Oscar Castilla. "Juez censura a Google y a medios que investigan a sindicado por narcotráfico." Ojo Publico. January 15, 2017. https://ojo-publico.com/351/juez-censura-google-y-medios-de-prensa-que-investigan-sindicado-por-narcotrafico [https://perma.cc/3XUR-AY86]

[379] California has a State Law ("erasure law") that allows for removal of content pertaining to minors; Brad Reid, Does the U.S. Need a Legal Right to Be Forgotten?, The Huffington Post, http://www.huffingtonpost.com/?icid=hjx004 [https://perma.cc/KV6U-2PJL]

[380] Eric Posner, *supra* note 155.

[381] Agatha M. Cole, *ICE Domain Name Seizures Threaten Due Process and First Amendment Rights*, ACLU (June 20, 2012) https://www.aclu.org/blog/ice-domain-name-seizures-threaten-due-process-and-first-amendment-rights [https://perma.cc/W7FX-Y4WH].

[382] Department of Justice, *Department of Justice Seizes More Than $896,000 in Proceeds from the Online Sale of Counterfeit Sports Apparel*, (April 10, 2012) https://www.justice.gov/opa/pr/department-justice-seizes-more-896000-proceeds-online-sale-counterfeit-sports-apparel [https://perma.cc/7VDM-PMY2].

[383] Mei Ning Yan, Protecting the Right to be Forgotten: Is Mainland China Ready?" EDPL (3) 2015 190 at page 194, https://doi.org/10.21552/EDPL/2015/3/6 [https://perma.cc/3N7L-7SES]

[384] *Id.* at 194, 195.

ISPs can be held liable for not following takedown procedures.[385]

Chinese law also contains criminal provisions under the Law on Administrative Punishments for Public Order (LAPPO) and the 2012 NPCSC Decision that govern the duties of the IPSs to protect online privacy and personal data.

The 2013 Guidelines set out standards for data controllers to follow while collecting, transferring or erasure of data.[386] Recently on November 7, 2016, the Standing Committee of the National People's Congress of China enacted the final Cybersecurity Law that will allow a data subject to request deletion of personal information that is incorrect, improper and contains errors.[387] This law will be in effect from June 2017.

Treatment of RTBF under existing law can be understood through a ruling by the Haidian District People's Court that referred to *Google Spain*. The petitioner's employment was terminated as he had an association with a company that had bad reputation, and consequently sued Baidu for lost wages and removal of his name from search results that showed the connection between the petitioner and the company. The court stated that the right of personhood can protect personal interest when "they must not encompass those rights which have already been categorized, and they must be rights which are both legitimate and which require protection."[388] The court rejected the petitioner's argument as the petitioner continued to work in the field and his association of the company was not incorrect.[389]

The Chinese legal system has not been examined for SSB laws and incidents in this Report. However, this is not an indication of the importance (or lack thereof) of the system.

b) Hong Kong

The collection of personal data is regulated under the Personal Data (Privacy) Ordinance which has been in operation since 1996.[390] In 2015, a court used this law to order removal of content comprising information about individuals in the financial market by a webmaster, David Webb. The data included court judgments of matrimonial disputes of those individuals dating back

---

[385] *Id.* at 195.

[386] *See Id.* at 198. Also *see* generally Law in China, Data Protection Laws of the World, https://www.dlapiperdataprotection.com/index.html?t=law&c=CN [https://perma.cc/P898-42EQ]

[387] *See Ron Cheng, China Passes Long-Awaited Cybersecurity Law, Forbes* (Nov. 9, 2016) https://www.forbes.com/sites/roncheng/2016/11/09/china-passes-long-awaited-cyber-security-law/2/#7a229c0532ee [https://perma.cc/U5JZ-DBU2] and *Final Cybersecurity Law Enacted in China,* Hunton & Williams, (Nov.8, 2016) https://www.huntonprivacyblog.com/2016/11/08/final-cybersecurity-law-enacted-china/ [https://perma.cc/7RPF-NMAZ]

[388] Fei Chang Dao, *An Overview of China's First "Right-to-be-Forgotten" Lawsuit*, (May 16, 2016) http://blog.feichangdao.com/2016/05/an-overview-of-china-first-right-to-be.html [https://perma.cc/W23J-AZ4G]

[389] Suhna Pierce & Adam Fleisher, *Europe's Right to be Forgotten Spreads to Asia,* (July 6, 2016) http://www.sociallyawareblog.com/2016/07/06/europes-right-to-be-forgotten-spreads-to-asia/ [https://perma.cc/W88T-D7KG]

[390] Law in Hong Kong, Data Protection Laws of the World, https://www.dlapiperdataprotection.com/index.html?c=HK&c2=&t=law [https://perma.cc/DK9H-YXAM]

to 2002.[391] After 10 years the courts decided to redact the names involved in the cases pursuant to a data subject's complaint and directed the webmaster to remove the names from his website. The webmaster refused to comply, and on appeal was held in violation of the data protection ordinance.[392] It is pertinent to note that the information was to be redacted from court orders, which are ordinarily public documents / public domain information but by virtue of this decision, these orders ceased to be "public domain" information.

c) India

There is no specific data protection law in India. India provides safe-harbors to intermediaries under the Information Technology Act, 2000[393] and the Copyright Act, 1957.[394] However, section 69A of the general act allows the government or any of its officers to issue orders to its agency or any intermediary to block access to information, including websites.[395]

Two cases that deal with RTBF arguments in different contexts with different results provide a picture of the uncertainty surrounding RTBF in India.[396] The Karnataka High Court directed its registry to redact the name of a woman from the order of the case. The woman had sought to annul a marriage certificate, but arrived at a compromise with the opposite side. The Karnataka High Court allowed the redaction resting its reasoning on the RTBF concept observing that it "*…is in line with the trend in Western countries of 'right to be forgotten' in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned*."[397] The court directed that the registry shall ensure that any Internet search made in the public ought not to reflect the name in the title of the case or the body of the case, however it noted that a certified copy of the order will contain the name.[398]

---

[391] *A Right to be Forgotten in Hong Kong?* Hogan Lovells, (Aug., 2015) http://www.hoganlovells.com/files/Uploads/Documents/Newsflash_A_Right_to_be_Forgotten_in_Hong_Kong_HK GLIB01_1452118.pdf [https://perma.cc/76PU-J7F8]

[392] Access Now Position Paper: Understanding the "Right to be Forgotten" Globally, (Spt.2016), https://www.accessnow.org/cms/assets/uploads/2016/09/Access-Not-paper-the-Right-to-be-forgotten.pdf [https://perma.cc/HZU4-RKBL] at 9, 10.

[393] *Shreya Singhal* (2015) India.

[394] Copyright Act, 1957, last amended by Act No. 27 of 2012 http://www.wipo.int/edocs/lexdocs/laws/en/in/in107en.pdf [https://perma.cc/F4HK-3JY3]

[395]The Information Technology (Amendment) Act, 2008, No. 10 of 2009, http://meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf [https://perma.cc/9TAP-PCHS] , (.. "in the *interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence"*)

[396] Kritikaccg, *Two takes on the Right to be Forgotten,* (Feb.24, 2017), https://ccgnludelhi.wordpress.com/2017/02/24/two-takes-on-the-right-to-be-forgotten/ [https://perma.cc/AJB3-3ECC]. (There are several other cases pending around different jurisdictions in India that may help shape the final stand of RTBF. Since the two judgements discussed here are from state courts and these courts, as well as the other jurisdictions, are corresponding benches, each decision is binding in its state. The other cases have not been included here because they are still pending.)

[397] *See Arunima Bhattacharya, In a First Indian Court Upholds the Right to Be Forgotten, (Feb. 3, 2017)* http://www.livelaw.in/first-indian-court-upholds-right-forgotten-read-order/ [https://perma.cc/269P-TJU5]. The order granting the relief is framed in this site.

[398] *Id.* at para 4 of the Order.

In contrast, the Gujarat High Court refused a petitioner's plea to restrict online databases and Google from publishing orders which are not "reportable," noting that anyone can get a copy of orders by applying to the court. The court rejected the argument that such publication is a violation of Article 21- Right to Life which includes right to privacy.[399] It is notable that any third party who wants to obtain court orders in cases can do so by applying to the registrar and stating reasons for the orders. The registrar normally has discretion to allow such applications.

With respect to SSB, there have been several cases of blocking of websites in India pursuant to orders by the Government. In August 2015, the government passed an order[400] to block 857 porn websites to protect "decency" and "morality."[401] Recently, Indian courts have issued several blocking orders against "rogue websites" that are primarily engaged in businesses that infringe intellectual property laws.[402] In one such instance, the Bombay court provided an order that displays compliance with several Manila Principles - It provides sample language for notice to be displayed in place of blocked website informing users of the relevant law under which the block is passed and also identifying an email ID for aggrieved users to contact. Further, the order notes that many SSB orders are overbroad and lack necessary temporal limits. Finally, it also notes that SSB orders are often passed without substantial proof of claim by the Plaintiff but this observation is unaccompanied by any guidance on what may constitute an adequate proof of claim.[403] This order is passed by a Single Judge of the Bombay High Court and has not been

---

[399] *See Ashok KM, Gujarat HC Rejects Plea to Restrain Websites from Publishing 'Non-Reportable- Judgment,* http://www.livelaw.in/gujarat-hc-rejects-plea-restrain-websites-publishing-non-reportable-judgment/ [https://perma.cc/Y2RM-W5CW]. The order: https://ia601501.us.archive.org/11/items/IndiankanoonGujHC/indiankanoon%20-%20Guj%20HC.pdf [https://perma.cc/EM5Y-QJR2].

[400] Notification No. 813/7/25/2011-DA (Vol. –V), Government of India, (July 31, 2015) http://www.thehindubusinessline.com/multimedia/archive/02496/DoT_Letter_3107201_2496720a.PDF [https://perma.cc/7XXG-QD5B].

[401] *Ban only on sites promoting child porn, says Centre*, THE HINDU, (Aug. 5, 2015) http://www.thehindu.com/todays-paper/tp-national/ban-only-on-sites-promoting-child-porn-says-centre/article7500711.ece [https://perma.cc/48M7-K4F3]. (The ban was restricted only to websites promoting child pornography, after public backlash against the government.)

[402] Star India Pvt. Ltd. v. Haneeth Ujwal & Ors., 2014 SCC Online Del 3837; Star India Pvt. Ltd. v. Roy Ma & Ors., 2014 SCC Online Del 2300; Fox Star Studios India Ltd. v. John Ceedge & Ors., 2014 SCC Online 1822; Novi Digital Entertainment Pvt. Ltd. & Anr. v. Five Desi & Ors. at http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=176887&yr=2016 [https://perma.cc/8XKS-R333]; Star India Pvt. Ltd. vs. Khalid Nasir Raja & Ors., at http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=59032&yr=2015 [https://perma.cc/LDM3-RPAG]; Star India Pvt. Ltd. v. Sujit Jha & Ors. at http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=240702&yr=2014 [https://perma.cc/5DDN-VBWL]; Fox Star Studios India ltd. v. Macpuler William & Ors. at http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=110404&yr=2015 [https://perma.cc/KJ5Z-LQ33]; In one such case, the Department of Technology appealed against the preliminary injunction as being overbroad. The appeal was dismissed by the appellate court applying similar principles as the UK courts. This court emphasised the importance of showing overwhelming evidence of infringement (Department of Electronics & Information Technology v. Star India Pvt. Ltd. at http://lobis.nic.in/ddir/dhc/PNJ/judgement/29-07-2016/PNJ29072016REVIEWPET1312016.pdf [https://perma.cc/BQ77-43BD]

[403] *Eros Int'l Media Ltd. v. BSNL, Suit (L) No. 751 of 2016, High Court of Judicature at Bombay, (Aug. 30, 2016),* https://spicyip.com/wp-content/uploads/2016/09/Bom-HC-order-in-Dishoom_-August-30.pdf [https://perma.cc/BZ9P-SZEE].

examined by a court of higher authority, yet.

d) Japan

The Japanese Supreme Court has recently decided a case in relation to deletion of internet search results, although there was no mention of "RTBF" specifically.[404] The case rejected a particular de-listing request, but indicated that such requests might succeed against search engines in other instances. The judgment follows the 2016 District Court ruling[405] that had decided the matter initially recognizing the EU RTBF. This decision was reversed by the Tokyo High Court which rejected the recognition of RTBF. While deciding in a case in favor of search engines like the High Court and not allowing deletion of search results regarding a person convicted under child prostitution and pornography laws, the Supreme Court relied upon privacy laws without discussing the recognition or lack thereof, of RTBF in Japanese law.[406] The Supreme Court has stated that the right of the public to have information outweighs the man's right to privacy. Justice Kiyoko Okabe is reported to have said that: "The deletion (of references to the charges from search engines) can be demanded only when value of privacy protection clearly exceeds freedom of expression of search sites."[407]

The report does not examine instances and laws concerning SSB in Japan.

e) Australia

With respect to SSB, Article 115A of the Australian Copyright Act prescribes injunctions against carriage service providers providing access to online locations outside Australia. In such cases, the Federal Court of Australia may, on application by the owner of a copyright, grant an injunction if the Court is satisfied that: (a) a carriage service provider provides access to an online location outside Australia; and (b) the online location infringes, or facilitates an infringement of, the copyright; and (c) the primary purpose of the online location is to infringe, or to facilitate the infringement of, copyright (whether or not in Australia).

It is pertinent to note that the Australian statute provides guidelines - a checklist of sorts - for a court to consider when ordering an injunction. Some of these facts include, whether disabling access to the online location is a proportionate response in the circumstances; the impact on any person, or class of persons, likely to be affected by the grant of the injunction; whether it is in the public interest to disable access to the online location, among others.[408]

---

404 *See Court decision may fire up 'right to be forgotten' debate*, The Japan Times, http://www.japantimes.co.jp/news/2017/02/02/national/crime-legal/court-decision-may-fire-right-forgotten-debate/#.WMmaeBLyvVo [https://perma.cc/CH8E-597X]

405 *Japan recognises 'right to be forgotten' of man convicted of child sex offences,* the Guardian, https://www.theguardian.com/technology/2016/mar/01/japan-recognises-right-to-be-forgotten-of-man-convicted-of-child-sex-offences [https://perma.cc/GT6T-ZB3U].

406 *Japanese court rules against paedophile in 'right to be forgotten' online case*, the Guardian, https://www.theguardian.com/world/2017/feb/02/right-to-be-forgotten-online-suffers-setback-after-japan-court-ruling [https://perma.cc/6MZV-QTPJ]

407 *Id.*

408 Section 115A (5), Copyright Act 1968, http://www.austlii.edu.au/cgi-

In 2016, the Federal Court ordered 61 domains registered to the websites The Pirate Bay, IsoHunt, TorrentHound and Torrentz to be blocked. Also, addresses belonging to SolarMovie were blocked.[409] Following the discussion in this Report, it is interesting to note that this order required a warning message to be displayed to users attempting to access the blocked website.[410] This message included informing the users that the website was blocked pursuant to a court order because it "infringes or facilitates the infringement of copyright."[411]

f) Europe and The United Kingdom

Since RTBF in Europe has been discussed in detail in Part III of the Report, it is not added in the Appendix to avoid repetition.

Like RTBF, Europe is amongst the most active jurisdictions in published SSB jurisprudence.[412] With the growth of the e-commerce industry, a number of these cases have addressed SSB via copyright and the sale of counterfeits and infringing products online. In fact, site-blocking has become a tool used commonly in Europe, including the UK.[413] Restrictions imposed by the EU have been issued based on courts' analysis of three directives: the IP Directive,[414] E-Commerce Directive[415] and the InfoSoc Directive.[416] In *Cartier*,[417] it was held that the underlying policy of the InfoSoc Directive permits restriction on entire websites *vide* intermediaries and that such restriction satisfies the proportionality test.[418] The court also

---

bin/sinodisp/au/legis/cth/consol_act/ca1968133/s115a.html?stem=0&synonyms=0&query=carriage [https://perma.cc/W2K3-68GB].

409 *Judge orders internet providers to block illegal downloading websites*, The Guardian, https://www.theguardian.com/technology/2016/dec/15/judge-orders-internet-providers-to-block-illegal-downloading-websites [https://perma.cc/55SD-SV2M].

410 Will Ockenden, & Jake Sturmer, *Internet companies forced to block The Pirate Bay, Bittorrent websites in Australia, Federal Court rules*, ABC News, (Dec. 15, 2016) http://www.abc.net.au/news/2016-12-15/federal-court-orders-pirate-bay-blocked-in-australia/8116912 [https://perma.cc/2963-BPSR]

411 *Id.*

412 The Telemedia Act, 2007 from Germany allows requests for filtering and removal of content sourced from third parties. Act CVIII of 2001 enforces the E-Commerce Directive in Hungary.

413 Section 97A of the Copyright, Designs and Patents Act 1988 in UK allows for and has been used to issue injunctions against service providers in trademark and copyright cases

414 DIRECTIVE 2004/48/EC OF THE European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (The IP Directive extends the InfoSoc Directive's mandate to intellectual property rights.)

415 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (The E-Commerce Directive allows injunctions on intermediaries by courts or administrative agencies, including orders for removal of/limiting access to illegal information.)

416 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (The InfoSoc Directive, surprisingly, notes intermediaries to be best placed to bring infringement activities to an end and provides right holders an opportunity to apply for injunctions to limit infringement of their copyright or related right)

417 *Cartier* (2016).

418 *Id.* at para 160-164.

emphasized the importance of considering all evidence before a restrictive order is passed.[419] The lower court's decision in *Cartier* provided for safeguards to prevent abuse of blocking orders:

a. If there is a material change in circumstances, target websites and ISPs may apply to courts for a discharge of the blocking order,
b. The page shown to users who try to access blocked content must include details such as names of parties that obtained the order and inform users of their right to appeal such an order,
c. When possible, such orders must carry a 'sunset' clause.[420]

In 2014, France passed a law allowing officials to ban websites that 'condone terrorism or distribute child pornography[421] without court orders.[422] This provision has been called vaguely worded and "equivalent to simply attacking the symptom of an evil rather than root cause."[423]

Spain passed the Sustainable Economy Act, commonly referred to as Sinde Law in 2012 that allows file-sharing websites to be blocked at the ISP level.[424] Few instances of the use of this law have been reported. It was used to block six sites for copyright infringement but the restriction was lifted by a Spanish court soon thereafter.[425]

Other instances of SSB have been seen in places such as Hungary that implemented a law in 2016 to block "illegal dispatcher services" in a move that appears to be aimed at Uber.[426] Similarly, the Turkish Government is known to frequently block access to social media during times of unrest.[427]

---

[419] *Id.* at para 158, ("In the context of this case, for example, the evidence also established that Richemont's brand names were famous and long standing; that these brands were a target of counterfeiters; that the operators of each of the target websites were offering and exposing for sale counterfeit copies of the products sold under just one of Richemont's brand names and that it was therefore hardly surprising that they had higher rankings (denoting that they were less frequently visited) than websites such as The Pirate Bay; that these activities and the activities of other counterfeiters cause significant damage to Richemont; and that the order sought would probably be highly effective.")

[420] *Cartier*, (2014) p. 262-265

[421] PRESS RELEASE, *France: Website blocking undermines freedom of expression,* (Feb. 16, 2016) https://www.article19.org/resources.php/resource/38257/en/france:-website-blocking-undermines-freedom-of-expression [https://perma.cc/VYG4-U9GN]

[422] Loppsi Act 2011.

[423] Press Release, France (2016) *supra* note 422.

[424] Spain; Law No. 2/2011 of March 4, 2011, on Sustainable Economy (as last amended by Law No. 2/2012 of June 29, 2012), http://www.wipo.int/wipolex/en/details.jsp?id=11977 [https://perma.cc/RS2G-39D2].

[425] *Spain lifts blocks on file-sharing websites*, BBC, (July 18, 2014), http://www.bbc.com/news/technology-28367990 [https://perma.cc/TG5W-TEAC].

[426] Hungary passes law that could block Uber sites, Reuters, (Jun. 13, 2016) http://www.reuters.com/article/us-uber-hungary-ban-idUSKCN0YZ1KD. [https://perma.cc/9N8M-H9DM]

[427] Cara McGoogan, *Turkey blocks access to Facebook, Twitter and WhatsApp following Ambassador's Assassination*, The Telegraph, (Dec. 20, 2016) http://www.telegraph.co.uk/technology/2016/12/20/turkey-blocks-access-facebook-twitter-whatsapp-following-ambassadors/ [https://perma.cc/49X4-XZXJ]; *Facebook, Twitter, YouTube and WhatsApp shutdown in Turkey*, Turkey Blocks, (Nov. 4, 2016)

https://turkeyblocks.org/2016/11/04/social-media-shutdown-turkey/ [https://perma.cc/JX99-GNTL] . *See also* *Yildirim* No.3111/10, (2012), ECtHR.

Appendix B: Reviewed Human Rights Documents

Introduction

This Appendix summarizes the human rights documents that were reviewed as research for the foregoing Report. These documents were selected based on their relevance to the issues surrounding intermediary liability and freedom of expression on the internet, with a focus on internationally binding and persuasive instruments, and those with high persuasive value in the OAS countries.

Each review summary begins with the title of the document reviewed, its author and year of publication. The reviews are arranged chronologically and also provide links to the document reviewed. Additionally, relevant paragraph/page numbers are provided in line with the discussion as identifiers.

A few other documents that were reviewed but not added in this Appendix due to their low relevance for the purpose of this report, as follows:

a. Freedom of Communication on Internet: Declaration adopted by Committee of Ministers (Dated May 28, 2003 at the 840th Meeting of the Ministers' Deputies)
b. Recommendation CM/Rec(2016)2 of the Committee of Ministers to member States on the Internet of citizens
c. Advisory Opinion of the Inter-American Court of Human Rights ("IACtHR"), regarding the compulsory membership in an association prescribed by law for the practice of journalism (1985)
d. Outcome Document of the "Connecting the Dots: Options for Future Action" Conference (August 10, 2015) (UNESCO)
e. Freedom of Connection Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet (William Dutton, Anna Dopatka, Michael Hills, Ginette Law, Victoria Nash) (2011)
f. European Parliament recommendation of 26 March 2009 to the Council on strengthening security and fundamental freedoms on the Internet

Background and Interpretation of the Declaration of Principles on Freedom of Expression, OAS, Office of the Special Rapporteur for Freedom of Expression (Edison Lanza)

Available at http://www.oas.org/en/iachr/expression/showarticle.asp?artID=132&lID=1 [https://perma.cc/DLJ2-GQQL]
Preamble available at http://www.oas.org/en/iachr/expression/showarticle.asp?artID=26&lID=1 [https://perma.cc/2VWH-4XPY]

The OAS Declaration of Principles on Freedom of Expression establishes a legal framework for the protection of free expression to be adopted by all states throughout the hemisphere. The Declaration states that OAS members are subject to Article 13 of the American Convention on Human Rights (ACHR), which provides for the "right to seek, receive and impart information and opinions freely," and sets forth principles that clarify how these rights apply to various forms of expression, journalistic activity, libel and slander laws, and monopolies in the media industry. In its accompanying interpretation of the Declaration, guided by the opinions of the Inter-American Commission (IACHR) and the Inter-American Court of Human Rights (IACtHr), the OAS calls for the incorporation of international standards on free expression and human rights into the Inter-American system.

Principle 1 states that freedom of expression is central to a free society and "includes artistic, cultural, social, religious and political expressions, as well as any other type of expression" (Paragraph 8).

Principle 2 establishes the right to receive, seek and impart information without discrimination. It notes that without equal access to information, people cannot take part in the democratic institutions of the state and their needs may not be accounted for in policy decision-making.

Principle 3 establishes the concept of habeas data writ, which gives people the right to undisturbed privacy, as well as the corresponding right to easily access information about themselves stored in public or private databases—without being required to provide a reason for doing so—and to correct anything that is erroneous, sensitive, biased, or discriminatory. The habeas data writ functions as an accountability mechanism, particularly for monitoring states that engage in illegal data collection or surveillance methods (Paragraph 14).

Under Principle 4, states have a duty to honor an individual's right to access information held by the state—that is, any official government documentation or information from a public source—because transparency is essential to civic participation and oversight. Under the "legitimate needs" test set forth by the IACtHR (Paragraph 20), access to state records can only be limited under exceptional circumstances that are "clearly established by law" in response to "real and imminent danger [to] national security."

Principle 5 prohibits all prior censorship of, interference with, or pressure exerted upon expression or the free flow of information. Here, as in its interpretation of other Principles, OAS cites the

IACtHR in defining prior censorship and recognizing the right of each person to express himself *and* to be well-informed (Paragraph 25). It also cites the Inter-American Commission's conclusions that state-imposed "limitations on the free flow of ideas that do not incite lawless violence" lead to the abuse of power (Paragraph 27).

Principles 6-9 focus specifically on journalistic activity. Principle 6 applies the above protections to journalists, citing the IACtHR's opinion that journalism depends on the right to free expression, which would be restricted if journalists were required to be members of professional organizations or to obtain a state license (Paragraph 30). Under Principle 7, conditioning the dissemination of information on its "truthfulness, timeliness, or impartiality" violates free expression by making the state the arbiter of the truth (Paragraph 31). Erroneous information produced with "actual malice" may be punishable, but only through the imposition of liability subsequent to the act of expression (Paragraph 35). Principle 8 establishes the right to confidentiality, which enables "every social communicator to refuse to disclose sources of information and research findings to private entities, third parties, or government or legal authorities" (Paragraph 36). Finally, Principle 9 affirms states' obligation to investigate, prosecute, and punish the "murder, kidnapping, intimidation of and/or threats to social communicators, as well as the material destruction of communications." Such acts eliminate those who investigate and report on abuses or illegalities and deter others from doing so, thus denying society its right to receive information (Paragraph 39).

Principles 10-13 deal with state influence over media laws and the media industry. Principle 10 establishes legal standards for balancing privacy rights and free expression in the enforcement of liberal or slander laws. Civil sanctions for violating such laws can only be imposed if, in disseminating news about public officials or people voluntarily involved in matters of public interest, a social communicator "had specific intent to inflict harm, was fully aware that false news was disseminated, or acted with gross negligence in efforts to determine the truth or falsity of such news" (Principle 10). Since libel or slander laws are often used to silence criticisms of public officials, this Principles places the burden of proof on individuals affected by the dissemination of false information to demonstrate that the disseminator did so with "actual malice," defined as "express intention to cause harm, with full knowledge that the information was false or with manifest negligence in the determination of the truth or falsity of the information" (Paragraph 46). Moreover, the state may not impose liability on someone who publishes information that is a value judgment, compel someone who criticizes public officials to verify their claims, or hold a third party that reproduces information responsible for its veracity (Paragraphs 47-49).

Principle 11 prohibits "desacato" [contempt] laws, which punish those that insult or offend a public official, since the scrutiny of public officials is a core pillar of democratic society (Paragraph 50).

Principle 12 states that monopolies or oligopolies in the media communications industry must be subject to antitrust laws, since control by a small group of individuals denies others equal opportunity to receive and impart information and limits the pluralism and independence of the media (Paragraph 53). Finally, Principle 13 prohibits state pressure, punishment, reward, or granting of privileges to social communicators based on their expressed opinions or approach to coverage, since such use of state power interferes with media independence, censors criticism of authorities, and impedes the free diffusion of information (Paragraphs 56-58).

Recommendation CM/Rec(2008)6 of the Committee of Ministers to Member States on Measures to Promote the Respect of Freedom of Expression and Information with Regard to Internet Filters, Council of Europe

Available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805d3bc4 [https://perma.cc/4A98-3DBJ]

This document is intended to provide Council of Europe member states with guidelines for their internet filtering policies. These guidelines are premised upon member states' general commitment to free expression, as well as previous Committee recommendations related to internet content. These include the need for common standards and strategies for transparency in information services, self-regulation and neutral labeling of searchable online content, the need for appropriate filters for content inappropriate for children, and the obligation to safeguard user privacy. The document builds upon the idea that users must be aware and able to use internet filters, and to challenge filtering and blocking of content, to seek for clarifications and remedies. The document is mostly focused on filtering policies, although it sometimes uses the words filter and blocking interchangeably.

Guideline 1 deals with user awareness of (and appropriate limitations on) internet filters. Specifically, it recommends that states notify users how filters work and why they apply to the content in question, as well as how these filters can be manually overridden if a user feels that the content has been blocked unreasonably.

Guideline 2 addresses appropriate filtering for children and young people, noting that such filters should be "intelligent" and adapt to a child's development over time.

Guideline 3 specifies the types of provisions that should be present in member states' internet filtering laws, such as effective means of recourse and remedy for improper filtering, and recommends that states not place general, overbroad filters on offensive and harmful content. Filters and blocks should not be universal and broad, and should only affect the group that the filter has been originally and specifically created to protect, and should not affect content that, while illegal in other contexts, is being used for legitimate purposes.

The Inter-American Legal Framework regarding the Right to Freedom of Expression, OAS, Office of the Special Rapporteur for Freedom of Expression (2010) (Catalina Botero Marino)

Available at *https://www.oas.org/en/iachr/expression/docs/publications/INTER-AMERICAN%20LEGAL%20FRAMEWORK%20OF%20THE%20RIGHT%20TO%20FREEDOM%20OF%20EXPRESSION%20FINAL%20PORTADA.pdf*
[https://perma.cc/3UUM-EWCV]

This report explains the general standards on freedom of expression supported by jurisprudence and doctrines binding in the Inter-American system while discussing their most pressing problems. It also lays an emphasis in showcasing best practices in the region and sets guidelines to help states shape their internal laws to Inter-American benchmarks.

The Special Rapporteur highlights the triple function that freedom of speech has been given in the Inter-American system as: (i) the right to think by ourselves and share our thoughts with others, (ii) the enabling right for a healthy democracy, and, (iii) a key instrument for the exercise of other fundamental rights (Paragraphs 6-10). When mentioning the scope of this right, the Report mentions that the right of an individual to express its own thoughts should be equally protected as the collective right of the society to receive that information. Therefore, a violation to the former cannot be justified using the latter or vice versa (Paragraphs 13-17).

As detailed by the Report, the range of activities covered by this right include the right to speak, write, disseminate, and produce artistic and symbolic expression. Also included is the right to seek, receive and have access to expressions, access to information about oneself and to possess information in any form (Paragraphs 19-29). In particular, the speech deemed in need of special protection is (i) political speech and speech involving matters of public interest, (ii) speech regarding public officials in the exercise of their duties and candidates for public office, and, (iii) speech that expresses essential elements of personal identity or dignity (Paragraphs 32-56).

The report also explains in detail the three-part test that must be observed to establish if a certain restriction on the exercise of freedom of speech is acceptable under the ACHR. This standard requires that the restriction should be clearly and precisely provided for by law (Paragraph 69); that it should be designed to achieve one of the vital objectives recognized in the Convention (Paragraph 74); and that it should be necessary in a democratic society to serve the compelling objectives pursued, strictly proportionate to the objective pursued, and appropriate to serve such compelling objective (Paragraphs 84-86). In any event, those limitations shouldn't be applied through prior censorship and can only be prosecuted after the dissemination of the information through the subsequent and proportional imposition of liability (Paragraph 91), cannot be discriminatory nor have discriminatory effects (Paragraph 93), and shouldn't be imposed by indirect means like the abuse of government controls or means tending to impede the communication and circulation of ideas and opinions (Paragraph 96).

It is particularly mentioned by the Report as a way of prior censorship proscribed by the Convention the order to include or remove specific links, or the imposition of specific content in Internet publications (Paragraph 148).

A Summary of the Study of Legal Provisions and Practices Related to Freedom of Expression, OSCE (2010) (Yaman Akdeniz)

Available here http://www.osce.org/fom/105522?download=true [https://perma.cc/HTA6-W4BD].

There are 56 members of the OSCE out of which 46 participated in this survey. The survey contained questions that would help ascertain existing legislative provisions for regulation of internet content and also related government practices. The study tried to ascertain the effect of the practices and regulations on freedom of expression. The four corners of the study are: internet access; internet content regulation; blocking, filtering, and content removals; and licensing and liability related issues, and hotlines to report illegal content (Page 14).

In relation to blocking, the study attempts to create a comparative analysis that contemplates:

1. legal provisions which require closing down and/or blocking access to websites or any other types of Internet content
2. legal provisions which require blocking access to web 2.0 based applications and services such as YouTube, Facebook, or Blogger
3. legal provisions requiring schools, libraries and Internet cafes to use filtering and blocking systems and software

Extraterritorial nature of the internet content is a major problem for regulation because: a. in many cases the content is hosted outside the territorial jurisdiction, and; b. The content may not be illegal in such outside territory given the cultural/political differences (Page 32). Due to this lack of harmonization of laws at an international level and the ineffectiveness of the local laws, governments have started to block content hosted outside the territorial jurisdiction- which is an easier and convenient "solution" (Page 33). Often, the blocking decisions are made by administrative bodies which are not transparent and sometimes without appeal procedure.

The study recognizes the importance Web 2.0 based platforms that contain legal content and the crucial role they play in enabling the public to participate in political discourse. It recognizes that the blocking/banning of access to entire website may have severe implications for political and social expression (Page 39). Further the study points out then-pending litigation referred to the CJEU from Belgium *(Scarlet Extended v Société belge des auteurs compositeurs et éditeurs* (Sabam), No 37/11) in relation to ISP level blocking/filtering which may impact fundamental human rights. Similarly, ECtHR was also considering two applications in the same area of contention (regarding the blocking of Google sites and Last.fm) which were expected to have a lasting impact on the European countries (Page 40).

While there are no requirements of using blocking software for certain type of content in most countries, Belarus, Croatia, Lithuania, Poland and Turkey, require filtering software to be used in academic institutions, libraries and Internet cafes. In other states, such as Canada, the Czech Republic, Hungary and Norway, the use of filters is voluntary and not subject to any laws or legal provisions (Page 41).

Amongst other, the study recommends in relation to blocking internet content that:

1. OSCE participating States should refrain from mandatory blocking of content or websites.
2. Voluntary blocking and content removal arrangements should be transparent and open to appeal.
3. Filtering should only be encouraged as an end-user voluntary measure.
4. Termination of Internet access based on "'three-strikes' measures to protect copyright is incompatible with the right to information.
5. Reliable information on applicable legislation and blocking statistics needs to be made available: The study specifically pointed out that the States should increase efforts to provide information.

General Comment No. 34 on Article 19 of the International Covenant on Civil and Political Rights, United Nations, Human Rights Committee (2011)

Available at http://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf [https://perma.cc/UL3Y-XPRW]

This General Comment offers guidelines to States on what the freedoms of opinion and expression mean in a series of current contexts. The Committee places a particular emphasis on explaining that the exceptions to Article 19 could be applied in accordance with the ICCPR.

The Committee says that the obligation to respect freedom of opinion and expression is binding on every part of the State as a whole (Paragraph 7), which means that it applies also to administrative agencies. At the same time, it draws a link between public and private action in light of the States' obligation to ensure that citizens are protected from any acts, including by private entities that may impair freedom of opinion and expression (Paragraph 7).

The Committee also interprets Article 19 broadly to cover freedom of opinion (a right with no restriction possible - Paragraph 9), freedom of expression (which covers even the expression considered as deeply offensive - Paragraph 11), its application in the media context (explaining that the public has a corresponding right to receive media output - Paragraph 13), the right to access information (Paragraph 18) and Freedom of Expression within the political rights context (Paragraph 20).

The General Comment explains in detail the scope and jurisprudence surrounding the possible restrictions to the freedom of expression and opinion, as established in Article 19(3) of the ICCPR (Paragraphs 21-35). These restrictions may relate either to (a) the rights and reputation of others, or, (b) to the protection of national security or public order. In particular, the Committee explains how these restrictions should concurrently be: (i) provided by a law that is available to the public, with enough precision to let everyone know what is not permitted (Paragraph 24); and (ii) necessary and proportionate for a legitimate purpose (Paragraph 33), which encompasses the obligation of States to individualize and demonstrate how a threat justifies an action. Regarding the subject matter for establishing restrictions, they could either be to (i) ensure the respect of the rights of others (Paragraph 28), or, (ii) to protect national security or public order (Paragraph 29).

The Committee specifically addresses the issue of electronic information dissemination systems, including internet service providers and search engines (Paragraph 43). In that regard, their General Comment mentions that any restriction to its operation could only be permissible as long as they are compatible with Article 19(3). Therefore, they should be only content-specific and, cannot be overarching bans on the operations of certain sites and systems or be ordered on the basis that they're critical to the government or their interests.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Document No. A/HRC/17/27 (May 2011) (Frank La Rue)

Available at http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/17/27 [https://perma.cc/V545-4M3R]

This report summarizes the findings of the Special Rapporteur that came from a series of communications, meetings, seminars, and country visits. The report highlights the fact that Article 19 of the UDHR and the ICCPR were crafted broadly enough to encompass freedom of opinion and expression on the internet and through other technological means. Categories of information that may be restricted include: child pornography, hate speech, defamation, direct and public incitement to commit genocide, and advocacy of national, racial, or religious hatred that constitutes incitement.

Chapter III of the report summarizes the first principles of freedom of expression in general and on the internet. It underlines the applicability of international human rights norms and standards on the right to freedom of opinion and expression to the Internet as a communication medium, and sets out the exceptional circumstances under which the dissemination of certain types of information may be restricted. Chapters IV and V address two dimensions of Internet access respectively: (a) access to content; and (b) access to the physical and technical infrastructure required to access the Internet in the first place. More specifically, chapter IV outlines some of the ways in which States are increasingly censoring information online, namely through: arbitrary blocking or filtering of content; criminalization of legitimate expression; imposition of intermediary liability; disconnecting users from Internet access, including on the basis of intellectual property rights law, cyberattacks, and inadequate protection of the right to privacy and data protection. Chapter VI contains the Special Rapporteur's conclusions and recommendations concerning the main subjects of the report." Chapters I, II, and V are not relevant for the purpose of this Report.

Arbitrary blocking or filtering of content (Paragraph 9-10)
This highlights the use of "just in time" blocking, which is censorship that prevents users from accessing or disseminating information during important political and social moments. The report mentions that "States' use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression," including because "blocking is not justified to pursue aims which are listed under article 19, paragraph 3, of the ICCPR, and blocking lists are generally kept secret, which makes it difficult to assess whether access to content is being restricted for a legitimate purpose" and blocks are "often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal" (Paragraph 31).

Imposition of Intermediary Liability
The European Union's E-Commerce Directive enables intermediaries to avoid liability for content if it does not have knowledge of illegal activity and removes it once it becomes aware. The Digital Millennium Copyright Act has similar provisions in the United States (Paragraph 41).

The report express concerns about notice-and-takedown regimes for two reasons. First, users whose content has been flagged for removal have little or no recourse. Second, intermediaries could err on the side of removal to avoid penalties, thereby censoring legitimate, legal content (Paragraph 42). The framework of "Protect, Respect, and Remedy" is based on three pillars: (1) States' duties to uphold human rights, (2) corporate responsibilities to do the same, (3) the need for victims to receive effective remedy (Paragraph 47). The rapporteur also emphasizes that restrictions of content on the Internet must comply with the three-Part Test (paragraph 69).

The Special Rapporteur highlights that any blocking or filtering of content should be accompanied with an explanation to users and to the operators of the websites that are blocked. The Special Rapporteur also calls for states to decriminalize defamation. Intermediaries should only be held responsible for removing content pursuant to legal orders issued by a court or "a competent body" that is independent of commercial and political influence (paragraph 70).

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Document No.: A/66/290 (August 2011) (Frank La Rue)

Available at http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf [https://perma.cc/TB7C-AFGB]

This report has been prepared pursuant to UN Human Rights Council (UNHRC) resolutions 7/36 and 16/4. The report deals with two aspects of the internet, access to content online and access to internet connection, with a focus on the types of expression that can be permissibly restricted by the State to comply with international human rights law. The Rapporteur recognizes the concerns in relation to privacy, specifically who collects personal information, the duration of storing such information and the way such information is used. The report refers to A/HRC/17/27 to highlight the Government's role in "fully protecting the right to privacy of all individuals" without which the right to freedom and expression cannot be enjoyed" (Paragraph 11).

The international law regime to protect right to freedom and expression is relevant in the age where technological advancement is fast, specifically under Articles 19 of the UDHR (Paragraph 14).

As mentioned in other documents, the Rapporteur reiterates the three "cumulative" criteria for compliance of international law that require any restriction on freedom of expression must (Paragraph 15):

1. be defined with sufficient precision so that an individual can regulate himself and must be publicly accessible,
2. comply with Article 19 paragraph of the ICCPR i.e. respecting the rights of others and protection of national security/ public order/ public health/ morals, and
3. be necessary and proportionate.

The Rapporteur recognizes that are different types of illegal content. Some content is mandatorily prohibited under international law. Other content may be considered harmful, offensive, objectionable or undesirable, but which States are neither required to prohibit or criminalize. Considering this, the rapporteur drafts a clear distinction between three types of expression:

1. expression that constitutes an offence under international law and can be prosecuted criminally;
2. expression that is not criminally punishable but may justify a restriction and a civil suit, and;
3. expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others. (Paragraph 18)

The types of expression that are required to be prohibited by international law are:

1. Child Pornography: The Rapporteur states that use of technology to block and filter the dissemination of such content should be precise and that there should be an independent and impartial regulating body to oversee and review. (Paragraph 22)
2. Direct and public incitement to commit genocide: The Rapporteur states that such acts should be prohibited by domestic law and the restrictions imposed by blocking or removing such content should be applied after an assessment of such expression (i.e. if the expression

is direct, public and with *mens rea* taking into consideration factors such as the speaker, meaning of the content, intended audience etc.) (Paragraph 25)

3. Advocacy of national, racist or religious hatred that constitutes incitement to discrimination, hostility or violence: As there is no definition of "hate speech" in international law, the Rapporteur emphasizes that context is central in determining whether an expression constitutes incitement (Paragraph 28). Accordingly, any restriction must be formulated in a way that clearly articulates its purpose to protect individuals from hostility, discrimination or violence (rather than protecting belief systems, religious or institutions from criticism) (Paragraph 30).

4. Incitement to terrorism: considering the broad definition of terrorism, the Rapporteur expressed concerns for the margin of discretionary power to interpret what kinds of expression constitute incitement to terrorism. (Paragraph 32)

The Rapporteur notes that one of the most used methods to restrict the prohibited expressions (as listed above) is blocking content and recommends that the State should provide full details about the necessity and justification of blocking content. Such blocking should be carried out by a judicial authority or body (with no political, commercial or other unwarranted influences) and should not amount to censorship. The rapporteur considers that generic bans on websites are not compatible with paragraph 3 of Article 19 and neither is blocking a website solely because the site has content that is critical of the government or of the political/social system the government fosters. (Paragraph 39)

Joint Declaration on Freedom of Expression and the Internet (1 June 2011) (Frank LaRue, Dunja Mijatović, Catalina Botero Marino, Faith Pansy Tlakula)

Available at http://www.osce.org/fom/78309 [*https://perma.cc/28GD-DYLD*]

Participating organizations: The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information (herein referred to as the "Organizations").

This document summarizes the main guiding principles and rules for promoting the freedom of expression agreed by and between the Organizations via the Joint Declaration on Freedom of Expression and the Internet (the "Declaration").

The Declaration is adopted by taking into consideration that: (a) freedom of expression is of significant importance for preserving democracy; (b) access to Internet is substantially growing, which gives access to information to billions of people and allocates power to the Internet to promote other rights and facilitate access to a variety of goods and services; (c) some governments restrict access to Internet; (d) restrictions to the freedom of expression shall be limited as envisaged by law for specific and limited reasons; (e) governments are not taking into account the specific nature of the Internet, which leads to restrictions of the freedom of expression, and last but not least; (f) there is a significant number of intermediaries (e.g. enabling access to materials posted by others, to financial and/or communication services), which are sometimes kept responsible for illegal content.

The Declaration outlines the general principles related to freedom of expression, and points out a variety of issues including Intermediary liability, criminal and civil liability, filtering and blocking, network neutrality and Internet access. The document uses the principles of the 'three-part test', impact assessments, internet literacy and the use of a tailored approach for regulation of the internet.

Intermediary liability: With respect to Intermediary Liability, the Declaration affirms the "Mere Conduit Principle" pursuant to which the intermediaries that provide technical Internet services such as providing access, or searching for, or transmission or caching of information shall not be deemed liable for content generated by others, if the intermediaries do not "*intervene in that content*" and comply with court orders to remove the content to the extent possible. Further, the intermediaries are not obliged to monitor content posted by others and "*should not be subject to extrajudicial content takedown rules, which fail to provide sufficient protection for freedom of expression.*"

Mandatory blocking & filtering: Mandatory blocking shall be used only in extraordinary circumstances (e.g. for protection of children against sexual abuse.) Content filtering, which is not

end-user controlled, shall not be used for restricting the freedom of expression, and the end-users shall be properly informed if end-user filtering option is available.

Criminal & Civil liability: Jurisdiction for cases related to Internet is determined on the basis of connection of the case with the States. The Declaration introduces: 1) the "Libel Tourism" rule, which envisages that private parties can only bring a case to the jurisdiction where they are able to "*establish that they have suffered substantial harm in that jurisdiction*", and 2) the "Single Publication" rule, which envisages "*damages suffered in all jurisdictions to be recovered at one time*."

Network Neutrality: the intermediaries shall provide access to their traffic or information management practices to all stakeholders. There shall be no discrimination of traffic based on source, destination or type of data transmitted.

Access to Internet: The Declaration envisages an obligation for the States to "*promote universal access to Internet,*" prohibit shutting down or slowing down of the Internet service, allow restriction to Internet for individuals only in exceptional circumstances and by court order. It proposes a positive obligation on States to adopt action plans for promoting Internet access, which shall include regulatory mechanisms, bringing awareness, envisaging special measures for disabled and disadvantaged people etc.

Joint Declaration by the UN Special Rapporteur for Freedom of Opinion and Expression and the IACHR-OAS Special Rapporteur on Freedom of Expression, UN and OAS (20 January 2012) (Catalina Botero and Frank LaRue)

Available at http://www.oas.org/en/iachr/expression/showarticle.asp?artID=888&lID=1 [https://perma.cc/8RVR-HQTJ]

Note: The previous document summarized was amended in 2012 to "*call on the United States to be vigorous in protecting freedom of speech on the Internet*" by the Special Rapporteur for Freedom of Expression of the IACHR, Catalina Botero Marino and the UN Special Rapporteur, Frank La Rue.

The Special Rapporteurs were particularly concerned about then-pending US legislation, the Stop Online Piracy Act (SOPA) and the PROTECT IP Act. Specifically, the creation of extrajudicial notice-and-termination procedures requiring a website to police user-generated content and targeting entire websites for even small portions of its content, that have potential impact on freedom of speech. At that time, the Special Rapporteurs were encouraged to see that Congress and the Obama Administration backed away from SOPA and reaffirmed they would not support legislation that reduces freedom of expression on the Internet.

Recommendation CM/Rec(2012)3 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Search Engines, Council of Europe

Available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa87 [https://perma.cc/ZSN2-JWFL]

This Recommendation predates the *Google Spain* "Right to be Forgotten" case, and highlights key concerns regarding free expression on search engines. The Recommendation appears contradictory in many respects, so - while it is an important snapshot for what the Council was thinking prior to *Google Spain* - it should be treated with caution.

The Recommendation acknowledges the significant role search engines play in collating and disseminating content on the internet. It advises states to allow search engines to perform this function. It notes, however, that search engines present risks to human rights by referencing content that is created by others. In particular, copyright and the right to a private life are cited as considerations for States in assessing "suitable regulatory frameworks" for giving protections to these "legitimate concerns" (Paragraph 3). The Recommendation is concerned about information that is "not intended for mass communication" (i.e., personal information).

In response, the Recommendation proposes that States engage with search engine providers to review search ranking and indexing of content which, although in the public space, is not intended for mass communication. . According to the Recommendation, this could be done by listing this content lower in its search results, with regard to the intentions or wishes of the person who produced the content ("broad dissemination as compared to content which is merely available in the public space"), including adopting default settings to achieve this (Paragraph 7).

This suggestion is in tension with the later statement that "search engine providers should not be obliged to monitor their networks and services proactively in order to detect possibly illegal content, nor should they conduct any ex ante filtering or blocking, unless mandated by a court order or competent authority" (Paragraph 13). The Recommendation anticipates that there may be legitimate requests (i.e., in relation to personal information) where search engines may be required to remove certain content from their indexes (Paragraph 13). Member States are advised to encourage search engine providers to develop tools to allow users to access, correct and delete data that search engines collected about them (Paragraph 11).

The Recommendation emphasizes that any de-indexing or filtering that is undertaken by search engines should be transparent, narrowly tailored and reviewed regularly with respect to compliance with due process requirements (Paragraph 14). The Recommendation anticipates blocking and filtering, but advises that this take place in a way that is transparent to users. Blocking of all search results should not be encouraged (Paragraph 16).

States are encouraged to work with search engines to develop self-regulatory codes, which protect individuals' fundamental rights, including due process, freedom of expression and privacy (Paragraph 18).

Although some limitations on complete transparency of search engines practices (i.e., explaining their algorithms so users can understand why certain results are returned or not) are acknowledged, the Recommendation support the cooperation between States, private sector and civil society to: encourage providers to enhance transparency in their results, especially if the results are not complete for any reason.

Considering the proliferation of audiovisual data, mobile Internet access, and face-recognition technologies, the Recommendation raises concerns about the impact of search engines on private life and data protection. The concern addresses the combination of information about an individual, creating an image "of a person that does not necessarily correspond to reality or to the image that a person would want to give of her- or himself" and imposing "a much higher risk for that person than if all the data related to her on the Internet remained separate." The recommendation mentions that "even long-forgotten personal data can resurface as a result of the operation of search engines" and that search engines should "promptly respond to users' requests to delete their personal data from (extracts of) copies of web pages that search engine providers may still store (in their "cache" or as "snippets") after the original content has been deleted." (paragraph 8).

Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services, Council of Europe

Available at *https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa9b* [*https://perma.cc/FP2L-7SKT*]

In this document, the Council of Europe Committee of Ministers highlights the public service value of social media and social networking sites, as well as their potential to pose a threat to human rights. According to the Committee, social networking sites inadequately protect children and young people from harmful content and lack privacy-friendly default settings. These social networking sites may provide a shelter to discriminatory practices by their weak/non-existent legal and procedural safeguards surrounding processes that lead to exclusion of users and due to the lack of transparency about personal data processing. Consequently, the Committee recommends that Council of Europe member states implement strategies for protecting human rights on social networking sites in accordance with the Convention for the Protection of Human Rights and Fundamental Freedom and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. In furtherance of this goal, the Committee outlines some general actions that member states can take, and also encourages public authorities and private sector actors to follow such action. These measures include raising user awareness of online human rights issues, promoting an environment that fosters free expression, increasing transparency about data collection and processing, and implementing self- and co-regulatory mechanisms to achieve these objectives.

The Committee lists some specific actions that states should take with respect to user rights, such as informing users about the default settings of their profiles and their rights to limit third party access to their contacts and information. Users should also be able to "opt in" to greater third-party access, to control how their personal information is published, to move and delete their data as well as withdraw consent to their personal data being processed, and to control their online identity (including through the use of pseudonymous profiles).

The Committee also recommends actions states should take with respect to protecting children from harmful content and behavior, such as responding to cyberbullying complaints, creating mechanisms for reporting inappropriate content, and cooperating with law enforcement authorities. It does not impose any specific legal obligations or liability on social networking sites for hosting harmful content, and notes that states should "refrai[n] from the general blocking and filtering of offensive or harmful content in a way that would hamper its access by users." (Paragraph 11)

Finally, the Committee provides a list of actions states should take to protect user privacy and promote awareness of social networking sites' data collection and processing methods.

Global Survey on Internet Privacy and Freedom of Expression, UNESCO (2012)

Available at http://unesdoc.unesco.org/images/0021/002182/218273e.pdf [https://perma.cc/U373-ENEM]

This document touches upon the relationship between the internet privacy and freedom of expression, and discusses various privacy issues arising from the use of the new technologies. It also provides information about the regulatory environment of Internet Privacy by comparing it with the freedom of expression. The Survey also discusses the national protection for privacy in China, Argentina, Mexico, USA, India, Egypt, France, Nigeria, and South Africa and outlines several useful resources that may be used to obtain more information about this topic (including for countries, such as: Africa, Europe and North America, Latin America, Asia). It also provides self-regulatory guidelines, normative challenges, policy recommendations and case studies. Among other key issues, it discusses the roles and the responsibilities of the service providers and intermediaries (e.g. Section 2.1.3 of the Survey).
The Survey acknowledges that internet-based communications rely more on the intermediaries for processing data, which leads to various concerns about the protection of privacy rights. It predominantly refers to the social networking sites, cloud computing capacities and search engines. It provides various examples for abuse of privacy by the intermediaries. For example: a) Internet Service Providers (ISPs) are coerced into "voluntary policing" the actions of their users; b) large transnational intermediaries negotiate with nation-states on seemingly equal terms due to their size and flexibility about their physical location, which leads to "pick and choose jurisdictions."

The Survey also acknowledges the privacy risks from the increased use of intermediaries and their control of personal data (Page 20). For example: a) cloud computing - poses a high risk to privacy due to unclear or vague terms of service of the cloud computing service. Further, data stored on clouds is accessible by multiple parties (including governments); b) Search engines – privacy issues surrounding search engines include cross reference of information between different service providers to build more exhaustive user profiles; c) Social networks – are most problematic because they tend to lock-in their users and often become irreplaceable. Social networking sites often unilaterally change their privacy policies, claiming that they informed their users and obtained consent. However, it is arguable that this stand is based on an incorrect assumption of the user's ability to understand and adequately consent to such policies. There are several other issues discussed by the survey including the potential mining of publicly available personal data on social networking sites etc. (Page 33).
The Survey outlines:

- The global standards for protection of privacy and personal data (e.g. Art.12 of the UDHR, Article 17 of the ICCPR, Article 8 of the ECHR),
- Several cases (e.g. Cases of Von Hannover v. Germany, cases before the ECtHR: Leander, Gaskin, Guerra, McGinley and Egan etc.)
- Regional standards on data protection, such as: the Organization for Economic Co-operation and Development (OECD), Asia-Pacific Economic Cooperation (APEC), Economic Community for West African States (ECOWAS), Organization of American

States (OAS), Council of Europe, EU Directive 95/46/EC.

Further, the Survey discusses the tensions between freedom of expression and privacy, the causes for such tensions (e.g. differences between privacy & data protection, different approach in Europe and USA).

The Survey provides various recommendations:

- Constitutional Protection - Strong constitutional protection for both privacy and freedom of expression. The Constitution must place clear limits on the scope of any restrictions to privacy.
- Civil Law Protection – a private remedy is envisaged against invasion of privacy that must cover information regarding which the user has reasonable expectation of privacy.
- Criminal Law Protection – sector-based criminal rules on privacy should be implemented to protect highly sensitive information (e.g. banking, telecommunication), as the right to freedom of expression shall be taken into consideration.
- Data Protection Systems – data protection regimes should be put in place, as exceptions shall be envisaged for the purposes of freedom of expression.
- Corporate practices – Corporations should develop strong privacy policies to protect their users. Self-regulatory measures are not recommended due to the business interests lining up against privacy. However, good business practices are considered essential for protection of privacy online (e.g. obtain efficient consent, clear privacy policies, control over privacy shall be given to the users).
- Raise awareness – States, corporations, civil society groups and media should raise awareness about privacy.

Freedom of Expression and the Internet, OAS Office of the Special Rapporteur for Freedom of Expression (2013) (Catalina Botero Marino)

Available at https://ccdcoe.org/sites/default/files/documents/OAS-131231-IACHR-ReportFreedomExpressionInternet.pdf [https://perma.cc/J63Q-H492]

This report identifies guiding principles for freedom of expression on the Internet and covers a number of issues including net neutrality, Internet access, cybersecurity, privacy, and Internet governance. It quotes and lists citations to other relevant human rights material. It identifies freedom of expression as a right with particularly strong protection in the Inter-American system (Paragraph 1) and reviews some relevant laws of some Inter-American states.

As a general matter, it says, Internet-specific remedies (Paragraph 12), must take into account "the impact the measure would have on the operation of the Internet as a decentralized and open network" (Paragraph 63) and the possibility of Internet-specific remedies such as rapid correction or response rights. (Paragraphs 64-71) Denial of Internet access radically violates freedom of expression (Paragraph 49). The report considers that the blocking of entire sites and services is "prohibited and exceptionally admissible" only strictly pursuant to human rights constraints, and affirms that blocks and filters should be should be "subjected to a strict balance of proportionality and be carefully designed and clearly limited so as to not affect legitimate speech that deserves protection" (Paragraphs 84-90).

The report deals extensively with Intermediary Liability. It states that intermediaries cannot be strictly liable for third party content, (Paragraph 95) and that intermediaries "must not be required to supervise user-generated content in order to detect and filter unlawful expression." (Paragraph 96) Strict liability or monitoring requirements would discourage existence of open platforms (Paragraph 97) and incentivize private censorship. (Paragraphs 98-99)

The report cites the "conduit principle" that intermediaries must not be liable for user content, "as long as they do not specifically intervene in that content or refuse to obey a court order to remove" it, (Paragraph 94) and at one point says liability should be imposed "only" on content authors. (Paragraph 102) It notes that, except in "extraordinarily exceptional" cases, requiring intermediaries to remove content based on notice from a private party creates incentives for private censorship. (Paragraphs 104-105) Removal processes should be subject to judicial safeguards: orders for removal should state precise location of content and provide transparency and access to remedies for the affected speakers. (Paragraphs 105-107) Mandatory blocking and filtering is permissible "in exceptional cases for clearly illegal content or speech that is not covered by the right to freedom of expression," (Paragraphs 85, 90) subject to stringent substantive and procedural tests (Paragraphs 86-88).

Notice and takedown systems "need to have certain requirements to be legitimate from the point of view of protection of freedom of expression." (Paragraph 97) The report also reviews other models such as notice-and-notice, (Paragraph 109) and notes that OSPs should always have opportunity to review and reject legal notices. (Paragraph 110) It also suggests that national law should enable transparency reporting. (Paragraph 113)

Addressing voluntary removals carried out under OSPs' discretionary policies, the report states that such measures must not arbitrarily limit free expression, and must be transparent and consistent with human rights principles. (Paragraphs 28, 110-112) and provide dispute resolution procedures (Paragraph 116).

The report provides more detailed focus on a few specific topics, including copyright (Paragraphs 75-83), jurisdiction (Paragraphs 66-88), and data localization (Paragraphs 173-74).

Fostering Freedom Online the Role of Internet Intermediaries, UNESCO (2014)

Available at http://unesdoc.unesco.org/images/0023/002311/231162e.pdf [https://perma.cc/9C3P-BX3G]

This report identifies freedom to express online as a right. It recognizes four principles as preconditions to internet 'universality': (1) human rights; (2) openness; (3) accessibility; and (4) multi-stakeholder participation (R-O-A-M) (Pages 9, 179). A part of the duty towards human rights includes the facilitation of the freedom of expression (Pages 15-18). The report identifies different types of intermediaries, using three major types as case studies – network providers, search engines and social networks (Page 22) to depict the impact of geopolitics, government regulation and company policies on user expression (Pages 58, 129). Using these case studies, it highlights difficulties faced by intermediaries in furthering free expression in jurisdictions where the governments are not inclined to implement policies towards internet universality. (Page 179)
For each case study, the report analyzes the company policies and practices of a few companies in different jurisdictions with respect to imposition of restrictions on free expression online. It elaborates upon: (a) the type of restrictions that the company may have to implement in the facilitation of free expression, including self-regulation by the company (Pages 62, 71,104, 107, 134, 136, 146), (b) the government attitude towards restriction of expression (Pages 66, 110, 138), (c) attitude of the company and the government towards data privacy (Pages 80, 119, 152), and (d) transparency policy and practice of the company and the government (Pages 70, 86, 123, 160).

The report recognizes that intermediaries play an important role in both the facilitation of free speech and the restriction of free speech. Restrictions can be implemented either by the intermediary or by the government, and can be broadly categorized as restrictions at the network-level, at the platform level and related to privacy (Pages 23, 24). The network level restrictions concern internet service providers, web-hosting providers and domain registrars. Search engines and social networks are able to implement platform level restrictions by removing content, limiting access to it or deactivating user accounts. Unlike the above restrictions, privacy related restrictions may be self-imposed by users that choose to limit expression online from the fear of data collection and monitoring, data interception and data exposure arising from varying levels of controls by platforms. (Page 24)

The report deals extensively with the regulatory framework of each analyzed country. It also highlights the public commitment by intermediaries to human rights principles, such as the Global Network Initiative (Page 26), Telecommunications Industry Dialogue on Freedom of Expression (Pages 59, 96) and Privacy and transparency reports (Page 10, 27).

The report stresses the need for an improved legal framework globally that would allow companies to frame their policies and practices better than the current framework (Page 168). For example, the report suggests that the commitment by companies in various countries is proportional to the commitment and threshold of liability implemented by the respective government (Pages 95, 138, 166). Further, the report advocates increased quantitative and qualitative transparency (Page 187). It states the need for implementation of guidelines (Page 167) such as the GNI recommendations for transparency (Page 129, 187) and the International Principles on the Application of Human

Rights to Communication Surveillance (Page 188). The report proposes that the industry dialogue would benefit in credibility by adding a process to verify compliance by committing companies/governments (Pages 129, 193). The report stresses the need for human rights impact assessments by governments and companies (Page 189). With respect to self-regulatory mechanisms, intermediaries can assist by:

1. Increased circulation of information
2. Establishing remedies to users such as public reports and explanations regarding actions that may violate human rights
3. Establishing their own grievance redressal channels. (Pages 92, 164, 189, 190)

The report also analyses gender biases on the internet and its impact on freedom of expression. (Pages 169-178)

Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a "Guide to Human Rights for Internet Users", Council of Europe

Available at
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000016804d5b31 [https://perma.cc/C5UP-K9HF]

This Recommendation focuses on how European countries should perform their obligations to protect citizens' human rights and fundamental freedoms on the Internet, in the context of the European Convention. Its central portion is a "Guide to Human Rights for Internet Users," a public awareness document to educate European citizens about their rights online.

The Council states that everyone whose rights and freedoms are restricted or violated on the Internet has the right to an effective remedy (Paragraph 99). They explain in detail that the remedies should be available, known, accessible, affordable and capable of providing appropriate redress (Paragraph 103) and that Internet users should be offered clear and transparent information regarding the means of redress available to them (Paragraph 105).

The Council notes that under the European human rights framework, the right to freedom of expression by Internet users and the right to reputation deserve equal respect and must be balanced. The Council also offers a list of criteria to strike this balance (Paragraph 41).

Regarding private companies acting as intermediaries, the Council says that it is possible for them to remove content created and made available by their users or even deactivate their accounts based on their Terms and Conditions. These actions would have to comply with the conditions of Article 10, paragraph 2, of the ECHR or they could be considered as an interference with the right to freedom of expression. (Paragraph 53)

Keystones to Foster Inclusive Knowledge Societies, UNESCO (2015)

Available at http://unesdoc.unesco.org/images/0023/002325/232563E.pdf [https://perma.cc/V2HP-GH4D]

This study collates conclusions from a research conducted with members of society, including governmental and non-governmental institutions. UNESCO highlights the necessity of Knowledge Societies, which are built on a free, open and trusted Internet that enables people to not only have the ability to access information resources, but to also contribute information and knowledge to local and global communities (Page 14). UNESCO identifies 4 fields which are keystones to building these societies, which are also within UNESCO's competencies: (a) access to information and knowledge, (b) freedom of expression, (c) privacy, and (d) ethical norms and behavior online. A table with components of each keystone is available on (Page 16). The UNESCO ROAM framework (described above in the summary of the *Fostering Freedom Online the Role of Internet Intermediaries UNESCO Report (2014)*) for Internet Universality, is emphasised. Definition of these principles is on (Page 17-18). The principles are a theoretical framework for the study, while the keystones represent the specific objects of inquiry to which the framework applies (related table at Page 18).

The report emphasizes that Article 19 of the UDHR applies to all platforms and all media. This provision is an enabler to the right of education and development. Many respondents and conference participants identified filters and blocks on content, whether imposed by governments or intermediaries such as ISPs or platform owners as inimical to freedom of access to information. Censorship of content, if it exists, should only be imposed as required to protect vulnerable populations (such as children) from content assessed as harmful to them. "Censorship, such as filtering or blocking of legitimate political speech, must be avoided" (Page 31).

Any limitation of freedom of expression online should be the exception rather than the norm. The international standard requires that any restrictions need to be enacted by law, should only be imposed for legitimate grounds as set out in the UDHR and ICCPR, and must also conform to tests of legality, necessity and proportionality (Page 38).

The report also discusses blocks, filtering and content regulation. The research showed that participants admit that there is a legitimate reason in some contexts to block certain content, such as material that incites violence. But this raises the question of how to draw the line in specific cases about what proportion, and with what transparency and redress mechanism. Numerous respondents to the consultation identified content restriction by governments as a major threat to freedom of expression (censorship of legitimate speech).

Another issue raised was the danger of holding intermediaries liable as if they were publishers. This may lead to intermediaries taking an overly aggressive proactive role in filtering content in response to formal or informal takedown requests (Page 42). The report discusses 'User Targeting and Profiling', i.e. users see different (customized) versions of the Internet depending on how algorithms use their previous searches and social media preferences. Such profiling may, happen at the government level, by private companies or even at an infrastructural level. Anonymity was

seen as an important tool to free expression (Page 43).

Respect for privacy (Pages 30-31, 59-62), Ethics (Page 10), and Data Protection and Surveillance (Pages 44-48) have also been discussed in this study. To promote privacy rights the report proposes, among others suggestions, the consideration of a Right to Be Forgotten (Page 62) as a practice of international relevance.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN (2016) (David Kaye)

Available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/38 [https://perma.cc/44AY-ZX9G]

This report, the first in a series concerning human rights in the digital age, focuses on the private sector. It lists key private actors in the Internet speech ecosystem, and identifies the UNHRC's Guiding Principles on Business and Human Rights as a framework for identifying their responsibilities.

In relation to Intermediary Liability, the report emphasizes the following trends:

- Vague speech regulation laws leading to over-censorship by individuals and businesses (Paragraph 39).
- Excessive intermediary liability laws leading to over-removal by intermediaries, sometimes because they are required to apply law to unclear claims. The Rapporteur linked this concern to the Right to Be Forgotten and the *Google Spain* case, stating that "the scope and implementation of this approach raises questions about the appropriate balance between the rights to privacy and protection of personal data on one hand, and the right to seek, receive and impart information containing such data on the other" (Paragraphs 40-44).
- Governments flagging content for removal based on companies' voluntary community guidelines, instead of based on court-adjudicated illegality (Paragraphs 45, 53). The Report's Conclusions state that governments must not disproportionately interfere with free expression by pressuring private companies to remove content without legal basis (Paragraph 85).
- The implementation of over-broad blocking and filtering. The rapporteur expressed concern about necessity and proportionality, and noted that filtering mandated in one jurisdiction may affect content not restricted in other jurisdictions (Paragraphs 46-47).
- Network or service shutdowns. The report noted that these have been observed in in many countries and are considered a "particularly pernicious means of enforcing content regulations" (Paragraph 48).
- Lack of appeal process for users whose content is removed under platforms' discretionary "TOS" standards (Paragraph 52) .

The Report urges increased transparency about content removals, from both state and private actors. (Paragraphs 63-66, 88-90). It also urges improved remedial or grievance mechanisms for Internet users affected by removal of their online expression. (Paragraphs 67-71).

Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, UN Human Rights Council (June 2016)

Available at http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20 [https://perma.cc/V545-4M3R]

The Resolution highlights the importance of protecting human rights, including freedom of speech, right to privacy and, equal opportunity to across genders and borders in enabling development and innovation on the Internet. The Resolution also highlights the need for promoting access to new technologies to persons with disabilities (Paragraph 7). Finally, the Resolution highlights the need for sovereign and global cooperation to enhance security on the Internet and promote trust amongst Internet users.

The Resolution calls for online rights equal to the rights that people have offline in accordance with the UDHR and the ICCPR (Paragraph 1). It affirms the importance of global cooperation in bridging various digital divides and the role of digital literacy in promoting right to education (Paragraphs 2, 3, 4, 5, 6). Condemning the violations of human rights committed on users for exercising their free expression on the internet, the resolution calls upon States to formulate transparent policies (including all stakeholders) and strengthen security measures on the Internet (Paragraphs 8, 9, 12).

Finally, the Resolution requests the High Commissioner to consult States, international organizations, communities, and industries to prepare a report on ways to bridge the gender digital divide. The High Commissioner is requested to submit the report at the thirty-fifth session. (Paragraph 13)

Privacy, Free Expression and Transparency: Redefining their Boundaries in the Digital Age, UNESCO (2016)

Available at http://unesdoc.unesco.org/images/0024/002466/246610E.pdf [https://perma.cc/4BLK-T5W3]

This report analyzes how the internet challenges the fundamental rights of privacy and free expression. In particular, it emphasizes tensions that arise from the interdependence and mutual support of privacy and free expression online (Pages 11, 77). The tensions between these rights on the internet are described in detail, and particularly the cross-border issues raised by the internet (Page 22).

When addressing the Right to be Forgotten, the report affirms that "for many, it is still debatable in the long run if this decision to remove what the court deemed as irrelevant and outdated information strikes the right balance between the two fundamental interests" (Page 28). An extensive analysis of the Right to be Forgotten indicates that many questions around the Google Spain case are still open, such as i) "who should balance the rights" of freedom of expression and data protection, i.e. whether it is proper to place the onus on an intermediary to decide whether to de-list data especially when the Google Spain decision does not provide clear guidance on this question, ii) what is the impact on smaller intermediaries and other online service providers (Pages 101-105). The report indicates that individuals' rights of access to information and freedom of information *must* be reconsidered in this digital age, "as when private institutions are gradually taking more public responsibilities and thus hold increasingly more personal information that is critical to individuals, the scope of this right is overly limited if it does not cover the information or data in possession of the private sector, public sector, and government bodies" (Page 28).

The report is based on the premise that human rights are equally applicable both online and offline (Pages 29-30). It describes, however, that there are key differences in how these rights are understood and upheld online by individual users, States and intermediaries. In particular, key risks to human rights include the erosion of user privacy (Page 13), increased opportunity for State surveillance through intermediaries (Page 17-18), and the lack of transparency by both State and non-State actors (Page 24).

The report emphasizes that the internet can be a tool that both facilitates and restricts free expression (Page 51). Internet intermediaries play a dual role in this: they enhance free expression, but this may also facilitate their own - or governments' - monitoring of individuals' online activities (Page 52). In light of the "critical status" of internet intermediaries in the operation of the internet, the report raises, as an example, a future need for tailored rules - that respect international human rights law - for governing the conduct of intermediaries. The report recognizes that arbitrary blocking poses a threat to freedom of expression, and also notes that such arbitrary blocking, filtering and censorship may be beyond necessity and proportionality where these activities are carried out in the name of national security. The report recommends sufficient legal safeguards to deal with the risks and challenges of this "merger" of data use for law enforcement, national security and intelligence service purposes (Page 115).

In its recommendations, the Report cites transparency as a key way of addressing the power of intermediaries in respect of free expression (especially for the so-called "internet giants" who, the report notes, are accountable to their shareholders rather than the public at large (Page 31). The report recommends that private sector and internet intermediaries consider introducing greater transparency measures wherever possible and appropriate, including that "terms of service and implementation of content moderation policies should be [...] transparent and narrowly-defined, and opportunities for redress should be offered" (Page 125).

The report recommends that internet intermediaries should be shielded from liability for third party content (118). The report further recommends (Page 122):

1. States should establish clear laws, following international standards, that keep restrictions on online free expression to a minimum.
2. States should enact sufficiently specific laws to define - proportionately - both the intermediaries' legal rights and their limited liability/responsibilities regarding privacy protection and free expression.
3. More breathing space be given to intermediaries to enable the thriving of free speech in general.
4. States should avoid Internet fragmentation, by refraining from controlling and separating national Internet spaces from the rest of the Internet (Page 123).
5. Intermediary self-regulation is recommended, within the framework of international human rights, where national legislation is not appropriate (Page 124).

Standards for a Free, Open and Inclusive Internet, OAS Office of the Special Rapporteur for Freedom of Expression (2017) (Edison Lanza)

Available at
https://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf
[https://perma.cc/8KVK-VUDW]

This Report was published as a chapter of the 2016 Annual Report of the Office of the Special Rapporteur for Freedom of Expression, and approved on March 15, 2017 by the IACHR. It represents the second and most recent thematic report that the OSRFE has issued devoted to the particular challenges presented by the Internet to freedom of expression since its *Freedom of Expression and the Internet* Report from 2013. This Report reprises and expands on the same underlying principles as the earlier document using new sources of interpretation and referring to contemporary debates like Network Neutrality, Internet Governance, and the RTBF

The Report is divided into four sections. The first section defines the four **Guiding Principles** that should inform a State's work, its policy-making activities, and the actions of private parties drawing from the recommendations of international bodies and certain national experiences. The first is the principle of a *Free and Open Internet*, understood both in terms of technical openness (interoperability) and also in economic terms (Network Neutrality) (Paragraphs 19 to 31). Next, the OSRFE highlights the principle of *Access to the Internet* as an enabling condition to the effective exercise of human rights and calls on states to take actions to progressively promote universal access, in terms of connection and digital literacy (Paragraphs 32 to 49). Among other concerns, the Report highlights the State's duty to guarantee the quality and integrity of Internet service, protecting it in all cases from arbitrary blocking, interference, interruptions, or slowdowns. Similarly, the Report then enshrines the principle of *Multi-stakeholder Governance* through the model of multilateral, transparent and democratic participation proposed by United Nations as a safeguard for human rights in Internet policy (Paragraphs 50 to 56). The fourth principle identified by the OSRFE is *Equality and Nondiscrimination*, defined as the State's obligation to address the specific Internet access needs that some particularly vulnerable groups, like racial or gender minorities, may have (Paragraphs 57 to 67).

The next section discusses the **Right to Freedom of Thought and Expression on the Internet**, as seen under the Inter-American system. The Report summarizes the current legal framework for freedom of speech as interpreted by the IACHR and the IACtHR, including the three-part test, the need to assign those decisions to an independent and impartial judge or court authority, the use of criminal law against speech and the role of privacy laws in relation to public interest information. Particularly, this section highlights the relevance of the Internet as a facilitator to the exercise of freedom of expression in all of its dimensions. About the site and service blocking debate, it states that any restriction on websites, blogs, applications or any other Internet-based electronic or other such information dissemination system or search engines, are permissible only to the extent that they are compatible with the conditions provided for the curtailment of freedom of expression. Although the OSRFE recognizes that certain blockings might be exceptionally admissible strictly pursuant to the terms of Article 13 of the ACHR, they should always include safeguards to prevent abuse, "such as transparency with regard to the content whose removal has been ordered, as well as detailed information regarding the measures' necessity and justification." On filtering, the

Report says that systems run by governments or commercial service providers not controlled by the end-user constitute a form of prior censorship and do not represent a justifiable restriction on freedom of expression.

This Report analyzes these principles in five areas. About the *Role of Private Sector*, the OSRFE calls upon private intermediaries on the Internet to put in place effective systems of monitoring, impact assessments, and accessible, effective complaints systems in order to identify actual or potential human rights harms caused by their services or activities (Paragraphs 85 to 101). Regarding *Intermediary Liability*, the Report says that a model of strict liability is incompatible with the ACHR because it is disproportionate and unnecessary in a democratic society. The Report leans towards a conditional liability model as long as it is respectful of the right to due process and other applicable guarantees (Paragraphs 102 to 120). On the issue of *Hate Speech on the Internet*, the Report takes the stance that blocking or filtering content to combat it should be a measure of last resort, used only be used when necessary and proportionate to the compelling aim pursued (Paragraphs 121 to 125). For the OSRFE, the *De-indexation and the "Right to Be Forgotten"* as a right recognized in the Costeja case is not based on international human rights law (Paragraphs 126 to 142). Moreover, the Report establishes clearly that "the application to the Americas of a private system for the removal and de-indexing of online content with such vague and ambiguous limits is particularly problematic in light of the wide regulatory margin of the protection of freedom of expression provided by Article 13 of the ACHR." Also, on the *Intellectual Property and Access to Knowledge* subsection, the OSRFE addressed the need to strike a balance between protecting copyright and protecting the rights to education, culture, and freedom of expression (Paragraphs 143 to 162). Particularly, the Report condemns several threats to freedom of speech derived from disproportionate enforcement regimes like disconnecting users, content filtering, criminal liability for non-commercial violations or blocking entire websites.

The third section covers the **Right to Access to Information**, as understood by the Inter-American system, and its exercise on the Internet (Paragraphs 163 to 182). The OSRFE puts an emphasis on the opportunities that the Internet opens for developing policies on proactive transparency and dissemination of information and ideas of all kinds, as well as the need to respect judicial remedies like *habeas data*.

Finally, the fourth section analyzes **the Internet and the Protection of Privacy and Personal Data** according to the international Human Rights standards (Paragraphs 183 to 265). For the OSRFE, the duty of ensuring freedom of speech is closely related to the protection of privacy as it is necessary for an individual to be able to freely form an opinion. Applying international law to current challenges, this Report discusses the protection of personal data; surveillance, monitoring, and collection; encryption and anonymity; "big data"; and the Internet of Things.