

DOSSIER

ENTRE EL DERECHO A LA VERDAD Y EL LLAMADO DERECHO AL OLVIDO: RETOS A LA DEMOCRACIA EN LA ERA DIGITAL

Catalina Botero Marino

Editora invitada

Everaldo Lamprea Montealegre

Editor general



Universidad de
los Andes
Colombia

Facultad
de Derecho



ESTUDIOS
JURÍDICOS
México

The Right to be Forgotten and Internet Governance: Challenges and Opportunities*

Christopher T. Bavitz

Harvard Law School, Cyberlaw Clinic
cbavitz@cyber.harvard.edu

Article received: June 22, 2018 | Accepted: July 27, 2018 | Modified: August 16, 2018

How to cite: Bavitz, Christopher T. "The Right to be Forgotten and Internet Governance: Challenges and Opportunities". *Latin American Law Review* n.º 02 (2019): 1-21, doi: <https://doi.org/10.29263/lar02.2019.01>

Abstract

This paper offers thoughts on the evolving nature and scope of Internet governance in the context of the development of the right to be forgotten. It summarises traditional frameworks for: (a) defining and operationalizing principles of Internet governance; and (b) distinguishing the types of issues that raise transnational governance concerns from the types of issues that are commonly considered the domain of local laws and norms.

If an issue falls within the ambit of Internet governance, it may lend itself to a certain set of solutions (with input from a broad cross-section of global public and private stakeholders). Issues outside that domain tend to be subjects of local regulatory mechanisms, in accordance with notions of national sovereignty. Categorizing a set of legal, policy, or technical considerations as one or the other, thus, has consequences in terms of the types of approaches to governance that may best be deployed to address them.

The paper provides examples of how recent technical and legal developments have put pressure on narrow conceptions of Internet governance as concerned primarily with Internet architecture and infrastructure. It posits that Internet governance models may be relevant to more and more

* Thank you to Catalina Botero Marino at Universidad de los Andes for hosting a conference in Bogotá, Colombia on the right to be forgotten in Latin America, in May 2017, that sparked important conversations about some of the issues addressed in this paper. Thanks also to Ryan Budish, Senior Researcher at the Berkman Klein Center for Internet & Society, for his valuable insights and feedback.

conduct that occurs above the level of Internet's metaphorical pipes, including developments that occur at what is traditionally conceived of as the content layer. The paper suggests that various global implementations of the right to be forgotten—and, in particular, implementations that are directed at the activities of search engines—offer a useful case study in examining and assessing this transformation.

Keywords

Right to be forgotten, internet governance, transnational governance, internet infrastructure.

El derecho al olvido y la gobernanza de internet: desafíos y oportunidades

Resumen

Este artículo contiene reflexiones sobre la naturaleza evolutiva y el alcance de la gobernanza de internet en el contexto del desarrollo del derecho al olvido. Resume los marcos tradicionales para (1) los principios que definen y hacen operativa la gobernanza de internet y (2) distinguir aquellas situaciones que implican preocupaciones transnacionales de aquellas que por lo general se consideran parte del dominio de las leyes y las normas locales.

Si una situación cae dentro del ámbito de la gobernanza de internet, puede prestarse para cierto conjunto de soluciones (con el aporte de una amplia sección transversal de actores interesados mundiales públicos y privados). Las situaciones que se encuentran por fuera de este dominio tienden a estar sujetas a mecanismos reguladores locales, en línea con las nociones de soberanía nacional. Por lo tanto, ubicar un conjunto de consideraciones jurídicas, políticas o técnicas dentro de alguna de estas categorías tiene consecuencias en términos del tipo de aproximación a la gobernanza que se puede emplear para abordar la situación.

Este artículo suministra ejemplos de cómo los desarrollos técnicos y jurídicos recientes han ejercido presión sobre las concepciones estrechas de *gobernanza de internet* que se ocupan principalmente de la arquitectura e infraestructura de la red. Plantea que los modelos de gobernanza de internet pueden ser relevantes más allá de lo que ocurre en las tuberías metafóricas de internet, e incluir los desarrollos que ocurren en lo que tradicionalmente se concibe como la capa de contenido. El artículo sugiere que varias implementaciones globales del derecho al olvido —y, en particular, implementaciones que están dirigidas a las actividades de los motores de búsqueda— resultan ser un estudio de caso útil para examinar y evaluar esta transformación.

Palabras clave

Derecho al olvido, gobernanza en internet, gobernanza transnacional, infraestructura de internet.

INTRODUCTION

The field of Internet governance (sometimes, “IG”) examines the design, regulation, and administration of the Internet’s infrastructure. Models of Internet governance offer processes and mechanisms to ensure consistency and interoperability of hardware and digital services across a broad and distributed network.

Online content sits on top of Internet architecture, and classic conceptions of Internet governance inherently contemplate—and are designed to accommodate—local and regional distinctions in approaches to the content layer. Different jurisdictions may (and often do) come to different conclusions about: (a) the extent to which particular forms of content are lawful or unlawful; (b) the roles, respectively, of users, platforms, service providers, and others in identifying and moderating online content; and (c) the responsibility—and, ultimately, potential liability—of parties in each of those roles with respect to such content.

Against this backdrop, the so-called right to be forgotten—perhaps more accurately described, in many cases, as a right to be delisted (“RTBF” or “RTBD”)—might be viewed as merely another local or regional approach to content regulation. One jurisdiction may differ from another to the extent to which it imposes (or limits) liability for intermediaries with respect to copyright infringement or defamation committed by their third-party content providers, describes the scope of permissible speech, or provides users of online services with a right to control the sharing of private information. Similarly, jurisdictions may differ in the rights they afford to individuals who are the subjects of online searches and the requirements that search engines must follow vis-à-vis the search results they deliver.

But, RTBF regimes pose more fundamental challenges to governance of the Internet than other forms of content regulation. That is due, in part, to the narrow regulatory underpinnings of the RTBF (which derives—in Europe, for example—from laws governing privacy and processing of personal data) juxtaposed with the broad impacts of the RTBF as implemented (which may permit individuals to manage the spread of truthful, but purportedly outdated or “irrelevant”, information about themselves). RTBF can pose especially thorny jurisdictional questions, depending on whether a given nation seeks to regulate (a) the processing of data within its jurisdiction; (b) the delivery of search results about a person within that jurisdiction to one conducting a search within that jurisdiction; or (c) the delivery of search results about a person within that jurisdiction to one conducting a search anywhere in the world.

This paper addresses some of the challenges posed by the right to be forgotten in the context of Internet governance. It proceeds from the assumption that, at the very least, the RTBF provides a useful case study of how cross-jurisdictional mechanisms that govern the technical and architectural layers of the Internet may co-exist with intra-jurisdictional mechanisms that regulate the content layer. The paper concludes with a call for decisionmakers to consider concerns about global governance in crafting laws and rendering decisions that interpret the right to be forgotten and its territorial impact.

LAYERS OF INTERNET ARCHITECTURE

Open communications systems and networks are often described using the conceptual framework of layers. The International Standards Organization’s Basic Reference Model, for example,

describes seven layers: the application layer, the presentation layer, the session layer, the transport layer, the network layer; the data link layer, and the physical layer.¹ Considered from bottom up —physical layer to application layer— each layer “sits ‘on top of’ the layers below it, and utilises the lower layers to perform its necessary function, with the ultimate goal being that information at the application layer is usable by the receiver in the manner intended by the sender”.²

With respect to the Internet, layers are sometimes conceived as taking the form of an hourglass: wide at the top and bottom and narrow in the middle.³ Jonathan Zittrain’s hourglass model positions the “Internet protocol” or “IP” layer —which incorporates fundamental rules governing the formatting and relaying of packets that is at the heart of online communications— in the middle of the hourglass, with applications on top and infrastructure below.⁴ Put succinctly, “[t]he shape of an hourglass inspired its selection as a metaphor for the architecture —the minimal required elements appear at the narrowest point, and an ever— increasing set of choices fills the wider top and bottom, underscoring how little the Internet itself demands of its service providers and users”.

These conceptions of the net underscore two things. First, they highlight ways in which various operational layers are separate (and thus amenable to different mechanisms for regulation and governance). Second, they highlight ways in which these layers are interrelated and function interdependently (such that a modifications at one layer may significantly impact other layers that build upon the modified layer).⁵

INTERNET GOVERNANCE

A. Traditional Conceptions of Internet Governance: Architecture and Infrastructure

Internet governance is concerned with “the processes, systems, and institutions that regulate things like TCP/IP, the Domain Name System, and IP numbers”.⁶ Approaches to Internet

1 International Organisation for Standardisation, *Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model* (ISO/IEC 7498-1, 2.^a Ed. 1994-11-14, corrected and reprinted 1996-06-15): 32-52, [http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994\(E\).zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip).

2 Robert A. Heverly, “Breaking the Internet: International Efforts to Play the Middle against the Ends: A Way Forward”. *Georgetown Journal of International Law* 42, n.^o 4 (2011): 1090, <https://ssrn.com/abstract=1825304>.

3 Committee on the Internet in the Evolving Information Infrastructure, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, *The Internet’s Coming of Age* (Washington, D. C.: National Academy Press 2001), 36. See Steve Deering, *Watching the Waist of the Protocol Hourglass* (Londres: IETF 51, agosto de 2001), <https://www.iab.org/wp-content/IAB-uploads/2011/03/hourglass-london-ietf.pdf>; Saamer Akshabi, Constantine Dovrolis, *The Evolution of Layered Protocol Stacks Leads to an Hourglass-Shaped Architecture (extended version)*, <https://www.cc.gatech.edu/~dovrolis/Papers/evoarch-extended.pdf>; Micah Beck, “On the Hourglass Model” (Arxiv.org, 25 de julio de 2015), <https://arxiv.org/abs/1607.07183>.

4 Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven: Yale University Press, 2009), 68, Fig. 4.1.

5 Committee on the Internet in the Evolving Information Infrastructure, Computer Science and Telecommunications Board, Commission Physical Sciences, Mathematics, and Applications, National Research Council, *The Internet’s Coming of Age* (Washington, D. C.: National Academies Press, 2001), 36.

governance “address technological design and administration, issues generally distinct from questions about content”. Examples of issues that relate to content, often conceived as outside the scope of Internet governance, include:

The economic and political implications of user-generated content, the politics of citizen journalism and blog content, new networked models of knowledge production, the political implications of the digital public sphere, and regulations about pornography.⁷

Models of Internet governance, thus, tend to focus on layers toward the bottom of the stack (or middle of the hourglass); the substance of Internet governance approaches tends toward the “invisible”.⁸

B. Expanding Conceptions of Internet Governance: Beyond the Pipes

The notion of Internet governance as intrinsically limited to the “technical layer of the network” can be needlessly limited and artificial.⁹ In light of the interdependence of the Internet’s layers, it can be difficult to distinguish in practice between the types of technically oriented considerations that lend themselves to consideration within the framework of Internet solutions and the types of content-oriented considerations that are ostensibly outside of IG’s bounds.

Consistent with a broader conception of IG, Laura DeNardis has proposed a taxonomy of the ecosystem that encompasses six functions:

1. The administration of critical Internet resources such as names and numbers;
2. the establishment of Internet technical standards (e.g., TCP/IP, HTTP);
3. access and interconnection coordination;
4. cybersecurity governance;
5. the policy role of private information intermediaries; and
6. architecture-based intellectual property rights enforcement.¹⁰

6 Lawrence B. Solum, “Models of Internet governance”, in *Internet Governance: Infrastructure and Institutions*, eds., Lee A. Bygrave y Jon Bing (U.K.: Oxford University Press, 2009), 50. In other words, Internet governance is the “broad ecosystem of institutions, laws, and private ordering that keeps the Internet’s infrastructure operational, as well as the enactment of public policy around this infrastructure”. Laura DeNardis and Francesca Musiani, “Governance by Infrastructure”, in *The Turn to Infrastructure in Internet Governance*, eds., Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson (Palgrave Macmillan, 2016), 4.

7 Laura DeNardis, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014), 20.

8 DeNardis and Musiani, “Governance by Infrastructure”, 5.

9 Anri van der Spuy, *What if we all governed the Internet? Advancing multistakeholder participation in Internet governance* (Unesco Publishing, 2017), 25. See Wolfgang Kleinwächter, *Towards a Holistic Approach for Internet Related Public Policy Making* (Global Commission on the Stability of Cyberspace Thought Piece, 2018), 7-8, <https://cyberstability.org/research/thought-piece-towards-a-holistic-approach-for-internet-related-public-policy-making/> (noting a move away from distinct “technical” and “political” layers and definition of Internet-related governance issues as “sectoral” problems).

10 DeNardis y Musiani, “Governance by Infrastructure”, 7, citing DeNardis, *Global War*.

Governance and regulation in the arena of privacy serves as a useful “case in point” concerning the blurring of lines between technical and policy infrastructure.¹¹ Global users of a global Internet have an interest in protecting the data and information they share against inappropriate transfer, receipt, and use by both private and government actors. A key component of managing online user privacy is technical, incorporating reference to design, architecture, and standards. But, individual nations (and—in the United States, for example—even individual states) may arrive at different policy conclusions about privacy regulation. Those different conclusions may address the extent to which users are best served by allowing users and online services to broker individualised privacy arrangements (e.g., the “notice-and-consent” framework that characterises much of online privacy law in the United States) or whether it is preferable to impose top-down requirements regarding data protection and limitations on data use (e.g., the General Data Protection Regulation framework adopted in 2018 in the European Union). As noted in a 2017 report from the United Nations Educational, Scientific and Cultural Organisation:

Privacy operates at all levels in an interconnected way, even if there may be fragmented governance - such as privacy regulation via data protection policies that operate in disjuncture with privacy-by-design in software development. It is for this reason that Internet governance is best understood as a holistic approach that extends beyond the technical dimension. The objects of governance decision-making may also vary, for example, from processes (technical standards, design of algorithms, deployment of encryption, Internet of Things (IoT) connections, etc.) through to people and their behaviours (e.g. bloggers, advertisers, engineers, government officials, privacy commissioners, etc.).¹²

If Internet governance mechanisms are meant to address “the design and administration of the technologies necessary to keep the Internet operational and the enactment of substantive policy around these technologies”,¹³ IG’s domain must include more than just the purely technical.

C. Why Does it Matter?

Two questions come to mind when examining these narrow and broad conceptions of Internet governance. The first (and, perhaps, most fundamental) question in framing the breadth of Internet governance is, why does it matter? Is the designation of a particular set of issues as within or outside the ambit of Internet governance purely a theoretical or semantic exercise? Or, does this designation have consequences? The answer is that defining a set of issues as within the scope of Internet governance may help to dictate or define a range of potential solutions available.

11 Van der Spuy, “What if we all governed”, 25.

12 Van der Spuy, “What if we all governed”, 25.

13 DeNardis, “The Global War”, 6.

1. Designation as Internet Governance Dictates the Tools of Regulation

One overarching purpose of identifying Internet governance as a distinct field of study and practice stems from a recognition that issues within the ambit of Internet governance lend themselves to tools and mechanisms designed to facilitate cross-border regulation of interconnected technical systems. Issues amenable to solutions rooted in Internet governance are proper subjects of technical design decisions, they fall within the domain of global institutions,¹⁴ may be fodder for international treaties,¹⁵ and benefit from multi-stakeholder approaches. Issues that fall outside the ambit of Internet governance, on the other hand, are generally conceived as the domain of local and national legal regimes (and of individuals and institutions that operate in accordance therewith).¹⁶

2. Examples: Regulation of Copyright and the Domain Name System

Two examples underscore the existence of differing governance approaches to IG and non-IG issues: administration of the “Domain Name System” or “DNS” (on the one hand) and regulation of copyright (on the other hand).

Computers connected to the Internet are associated with strings of numbers that serve as identifiers. Text-based domain names “make it easier for humans to remember” those identifiers.¹⁷ The management of the global system of domain names and the connection of those names to the numbers that describe the location of data and information on the World Wide Web represents perhaps the paradigm example of a set of regulatory considerations amenable to Internet governance approaches. The DNS could not function were it left entirely to the discretion of local regulators (and businesses operating pursuant to local laws) to proscribe and implement a system. Instead, a set of global standards has been developed, implemented under the auspices of ICANN and IANA to manage both the allocation of top-level domains or “TLDs” and the primary DNS root service.¹⁸ The centralised administration of DNS reflects

14 These include institutions such as the Internet Corporation for Assigned Names and Numbers (“ICANN”), the Internet Assigned Numbers Authority (“IANA”), and standards-setting organisations like the World Wide Web Consortium, the Internet Engineering Task Force, the International Telecommunication Union, and the Institute of Electrical and Electronics Engineers. DeNardis, “The Global War”, 22.

15 DeNardis, “The Global War”, 23.

16 This does not suggest that governance of the Internet falls entirely outside the domain of local legislation or regulation or that national laws cannot reach conduct online, as may have been suggested by John Perry Barlow’s 1996, *A Declaration of the Independence of Cyberspace*. See John Perry Barlow, “A Declaration of the Independence of Cyberspace”, *Electronic Frontier Foundation*, February 8, 1996, <https://www.eff.org/cyberspace-independence>; see also Lee A. Bygrave and Terje Michaelsen, “Governors of Internet”, in *Infrastructure and Institutions*, eds., Lee A. Bygrave and Jon Bing (New York: Oxford University Press, 2009), 115. Indeed, models of Internet governance expressly contemplate a role for national governments. See Bygrave and Michaelsen, “Governors”, 117-125.

17 Lee A. Bygrave, Susan Schiavetta, Hilde Thunem, Annebeth B. Lange, and Edward Phillips, “The naming game: governance of the Domain Name System”, *Infrastructure and Institutions*, eds., Lee A. Bygrave y Jon Bing (New York: Oxford University Press, 2009), 147.

18 Bygrave, Schiavetta, Thunem, Lange, and Phillips, “The Naming Game”, 149-156.

an effort to promote consistency and stability with respect to the ability of individual Internet users to access content and information stored on servers throughout the world using consistent sets of names and numbers.

Copyright law is territorial, and questions about the scope of copyright protection, rights ownership, and availability of individual protected works for licensing are dictated by local law and by the business priorities and interests of licensors and licensees. One seeking to launch an on-demand streaming music service (along the lines of Spotify) must consider the protections for sound recordings and musical compositions and the individual bundles of rights therein (including rights of reproduction and performance), and must specifically consider those issues separately in each country. Copyright owners considering rights enforcement must be guided by local laws that prescribe and define their rights. And, copyright users must similarly adhere to local regulations that govern licensing and the viability of defences to infringement (including fair use). In brief, global copyright licensing—particularly for entities that operate across national borders—presents issues that are thorny but that are not among those one might typically consider to be within the scope of Internet governance. Inconsistencies in laws and business practices across borders raise complexities for licensees, but those complexities are largely considered an inherent part of doing business in a field governed by local, territorial legal regimes.

Treaty obligations may inform local regulation in non-IG arenas such as copyright. But, the primary source of authority on these types of issues remains local, rooted in government institutions. Outside the ambit of IG, a premium is placed upon the ability of such institutions to respond to and take into consideration local values and norms in crafting viable governance structures. Issues that lend themselves to consideration within IG frameworks, on the other hand, lend themselves to structures that integrate influences from a wide array of local and global actors.

D. Is There a Limiting Principle?

A second question concerns whether some limiting principle might constrain expanding concepts of Internet governance. That is, if IG addresses not just technical architecture but certain aspects of the content layer as integrated with network design and infrastructure, could we say that Internet governance encompasses all issues of regulation online?¹⁹

There is certainly a risk of governance creep as Internet governance models are extended to reach beyond the Internet's infrastructure layers. If IG is everything, IG is nothing. But, there are practical ways to define those circumstances in which Internet governance frameworks may be of use.

For example, a “complete”—neither overbroad nor excessively narrow—conception of Internet governance is characterised by a *“focus on the nexus between Internet architecture*

19 As noted by Lawrence Solum: “If the topic of Internet governance were taken as the investigation of the regulation of all these activities when they took place on (or were significantly affected by) the Internet, then ‘Internet governance’ would be more or less equivalent to ‘law and politics’ at least in the ‘wired’ and ‘wireless’ (or more developed) nations. This definition of Internet governance is simply too broad and ill-defined to be useful for the purposes of this investigation”. Solum, “Models” 49.

and social policy".²⁰ It is neither the architecture nor the content but the connection between the two that suggests that IG and its suite of multi-stakeholder approaches may be of use.

In addition, Internet governance frameworks —as opposed to frameworks rooted solely in local or national legal systems— may be viewed as especially applicable not just to infrastructure (writ large) or content (writ large) but to any set of issues that is poorly suited to resolution by local or national government institutions. That might include issues on which governments and political institutions either cannot intercede or do not desire to do so, perhaps because they are overly technical, perhaps because they raise cross-border concerns that a single nation's institutions are unable to fully address.

THE RIGHT TO BE FORGOTTEN

A. Overview

In its various forms, the “right to be forgotten” aims to address a vital and timely concern, “namely, the Internet’s ability to preserve indefinitely all its information about you, no matter how unfortunate or misleading”.²¹ “The ‘right to be forgotten’ refers to the right of an individual to erase, limit, or alter past records that can be misleading, redundant, anachronistic, embarrassing, or contain irrelevant data associated with the person, likely by name, so that those past records do not continue to impede present perceptions of that individual”.²² Attempts to implement the right to be forgotten inherently involve attempts to balance competing rights of free expression (specifically, the right to convey, and receive, truthful information on matters of public concern) and privacy (specifically, the right to restrain sharing of information deemed unduly personal or sensitive in a manner that might cause harm). Frameworks for implementing the RTBF draw on local norms and derive from local mores in their efforts to achieve such balance.

20 Solum, “Models”, 52 (emphasis in original). Solum posits that Internet governance is concerned with “both narrow issues implicated by the institutions that govern the technical infrastructure and architecture of the Internet and the broader issues that are implicated by the ways in which the Internet transforms policy questions that directly implicate applications, communication, and conduct” and argues that “[b]ecause the narrow issues are rarely of substantial intrinsic importance (architectural elegance of network design matters only to network engineers) and the broad issues are sometimes of great social importance (fundamental human rights matter to everyone), it is important that investigations of Internet governance focus on the relationship between technical infrastructure and Internet architecture and the impact of the Internet on broad policy questions”. Solum, “Models”, 51-52.

21 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>.

22 Michael J. Kelly and David Satola, “The Right to be Forgotten”, *University of Illinois Law Review* 2017, n.º 1 (2017): 3, <https://illinoislawreview.org/print/volume-2017-issue-1/the-right-to-be-forgotten/>, citing Cécile de Terwangne, “The Right to be Forgotten and Informational Autonomy in the Digital Environment”, in *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten*, eds., Ângela Pereira, Alessia Ghezzi, and Lucia Vesnic-Alujevic (Palgrave MacMillan, 2014), 83-84.

B. The Right to Be Forgotten in the European Union—The Google Spain Case

The right to be forgotten in its most fully realised form stems from a European Commission Directive and a widely-publicised 2014 European Court of Justice case that interpreted it. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals concerns “the processing of personal data and on the free movement of such data”.²³ Directive 95/46 confers rights on the subjects of data (including rights to access and request erasure of that data) and obligations on so-called data controllers with respect to those data subjects’ rights.

In *Google Spain SL v. AEPD*, Case C-131/12, May 13, 2014 (“*Google Spain*”, sometimes referred to as the “*Costeja*” case), the European Court of Justice held that—with respect to search engines—the rights and obligations conferred by Directive 95/46 include a right of data subjects to be free from data that are “inaccurate”; “inadequate, irrelevant or excessive in relation to the purposes of the processing”; “not kept up to date”; or “kept for longer than is necessary”.²⁴ In practical effect, the *Google Spain* case recognises a “right to be forgotten” (or, more appropriately, a “right to be delisted”), meaning that individuals who are the subjects of search results that point to information that has these characteristics may request that such search results be removed. The case is “indicative of a more general trend, followed by the European Union legislature and spurred by the emergence of the digital economy, leading towards a stronger protection of the fundamental personal rights conferred upon physical persons, or so-called ‘data subjects’, and exercised against entities making use of their data for their own purposes”.²⁵

Article 94 of 2018’s Global Data Privacy Regulation (“GDPR”) expressly provides that “Directive 95/46/EC is repealed with effect from 25 May 2018”.²⁶ The GDPR codifies the right to be forgotten as a right against data controllers to “erasure of personal data”, with express exceptions for data processing that is necessary, among other things, “for exercising the right of freedom of expression and information” and “for archiving purposes in the public interest...”.²⁷

23 Official Journal of the European Communities. “Directive 95/46”. Official Journal L 281/31. November 23, 1995.

24 Court of Justice of the European Union. *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12)*. May 13, 2014. The reference to data kept longer than necessary recognises that some types of data “are required to be kept for historical, statistical or scientific purposes”. Directive 95/46 at Article 29.

25 Michel J. Reymond, “Hammering Square Pegs into Round Holes: The Geographical Scope of Application of the EU Right to be Delisted”, *Berkman Klein Center for Internet & Society, Research Publication*, n.º 2016-12 (2016): 1, <http://dx.doi.org/10.2139/ssrn.2838872>.

26 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art. 94 (Apr. 27, 2016).

27 GDPR, Art. 17.

C. Other Conceptions of RTBF—Hosts v. Search Engines

The *Costeja* case highlights—and focuses on—the effects of search engines as distinguished from the publishers of websites linked to in search results. The ECJ expressly noted in *Costeja* that search engines “play[] a decisive role in the overall dissemination” of data hosted by publishers and renders those data “accessible to any internet user making a search on the basis of the data subject’s name, including to internet users who otherwise would not have found the web page on which those data are published”.²⁸ The decision thus implements one particular mechanism for vindicating privacy rights of the subjects of information published on the web by focusing on the role that search engines play both in: (a) drawing attention to a given article, and (b) connecting that article to the name of a claimant asserting his or her right to be forgotten.

Other conceptions of the RTBF focus more squarely on the online publishers themselves. A pair of pre-*Costeja* decisions from the Colombian Constitutional Court involving Colombia newspaper, *El Tiempo*, for example, approach the types of concerns at the heart of the EU’s right to be forgotten regime in a manner that addresses the conduct of the paper in maintaining older news articles online without updating them to reflect recent developments. In *Gloria v. Casa Editorial El Tiempo*, T-277/15, May 12, 2013, the Court held that a newspaper was obligated to update a story to reflect claimant’s acquittal on criminal charges.²⁹ In *Martínez v. Google Colombia & El Tiempo* publishing house, Judgment T-040/13, January 28, 2013, the Court held that the newspaper was responsible for updating information in a story that reported claimant’s name had come up in a criminal investigation but did not note that he was convicted of no crimes.³⁰ In both cases, the Court held that the responsibility fell to the newspapers and not to search engines (like Google) that direct searchers to those online news stories.

Some European courts have taken a similar approach, post-*Costeja*. In *P.H. v. O.G.*, Belgian Supreme Court, 29 April 2016, ref. C.15.0052.F; for example, the Belgian Court of Cassation held that—in order to protect claimants’ privacy interests, asserted within the context of the post-*Costeja* right to be forgotten—a newspaper should remove the name of the RTBF claimant from an archived article about his past unlawful conduct.³¹ The Court expressly addressed the role of search engines in drawing attention to the article in question, a role deemed so central by the ECJ in *Costeja*. But, the Court concluded that any harm caused by search engines in connecting the claimant to the archived article was based on the newspaper’s inclusion of the claimant’s name in that article.

These alternative approaches to issues at the heart of a *Costeja*-style right to be forgotten recognise the limited role that search engines play in directing web users to information online.

28 *Google Spain SL v. AEPD*, Case C-131/12 (May 13, 2014), Par. 36.

29 *Gloria v. Casa Editorial El Tiempo*, T-277/15 (May 12, 2013). See <https://wilmap.law.stanford.edu/entries/constitutional-court-gloria-v-casa-editorial-el-tiempo-t-27715>.

30 *Martínez v. Google Colombia & El Tiempo* publishing house, Judgment T-040/13 (January 28, 2013). See <https://wilmap.law.stanford.edu/entries/constitutional-court-martinez-vs-google-colombia-el-tiempo-publishing-house-judgment-t>; <https://globalfreedomofexpression.columbia.edu/cases/martinez-v-google/>.

31 Belgian Supreme Court, *P.H. v. O.G.*, April 29, ref. C.15.0052.F. See <https://globalfreedomofexpression.columbia.edu/cases/p-h-v-o-g/>; <https://wilmap.law.stanford.edu/entries/belgian-supreme-court-29-april-2016-ref-c150052f>.

But, focusing on the source raises significant concerns in the context of free expression. Compared with an approach that addresses modifications to search results, “[d]eleting information at its source does ... more harm, potentially eliminating it from the Internet completely”.³²

INTERNET GOVERNANCE AND THE RTBF: OBSERVATIONS, CHALLENGES, AND OPPORTUNITIES

A. Overview

As noted above, traditional approaches to Internet governance suggest that: (a) there is value in pursuing multi-stakeholder, inter-disciplinary technical, business, and legal approaches to core technical interoperability considerations; and (b) local (or national) approaches, recognizing local (or national) values and mores, may be more appropriate when applied to questions about the substance of online content. The more RTBF regimes are concerned with content (as they surely are, to some extent, insofar as they seek to provide remedies for online materials that are out-dated or inaccurate), the more they are properly subjects of local regulation and have little to no relevance in the context of Internet governance. On the other hand, the more concerned they are with technical interoperability (as they surely are, to some extent, insofar as they seek to leave content in place but disrupt search mechanisms that accurately identify and point to information online), the more they may benefit from consideration within an Internet governance framework. This section addresses three features of RTBF regulation —none unique to the context of RTBF but all implicated thereby— that: (a) underscore ways in which RTBF tests the limits of these traditional dichotomies, and (b) mitigate in favour of considering global governance concerns in the context of RTBF.³³

B. Search Engines—Twin Functions as Information Location Tools and Speakers

Part of the complexity of fitting RTBF into an Internet governance framework involves the twin roles of search engines both as information location tools (linking to the content of other speakers and publishers online)³⁴ and as speakers themselves (effectively expressing the views

32 Daphne Keller, “The Right Tools: Europe’s Intermediary Liability Laws and the EU 2016 General Data Protection Regulation”, *Stanford Law School Center for Internet and Society*, (2017): 35, <http://dx.doi.org/10.2139/ssrn.2914684>.

33 This section focuses primarily on the role of search engines and on models for implementation and enforcement of RTBF geared not toward underlying information content providers but, rather, toward platforms that facilitate search and direct Internet users to online content.

34 The term “information location tools” has salience in the context of copyright law, but it may have broader application as well. Section 512 of the United States Copyright Act addresses “information location tools” in the context of establishing their liability (or immunity therefrom) in the context of the Act’s intermediary liability and safe harbor regime. See 17 U.S.C. § 512(d) (referring to “information location tools” as “referring

of search engine operators as to the relevance and propriety of links in the context of a user's search). The former feels more like the type of function one might traditionally expect to lend itself to solutions that incorporate global governance frameworks. The latter feels more like the type of speech regulation one might traditionally expect to be a subject of local law.

But, even the activity of a search engine in connecting a user's searches to relevant links is not the same sort of relatively straightforward, one-to-one matching exercise employed by the Domain Name System in correlating URLs (entered as text strings) to the numbers that identify the location of content. Indeed, the results proffered by search engines inherently involve value judgments and determinations of relevance that go far beyond the sorts of technical functionality at the heart of DNS. One searching for the English word "bass" may be searching for information about a species of fish or about a low-tuned stringed musical instrument.³⁵ One searching for an individual's name may seek biographical information; data on the search subject's whereabouts; or expressions of opinion about the individual's character or credentials sufficient to vet the search subject as a potential babysitter or political candidate.

Evaluating relevance requires the search engine to parse the searcher's intended meaning. This may involve a complex assortment of context clues (e.g., the "bass" searcher in the past has sought information about sport fishing, or has entered the search term at a time when a highly-publicised documentary about renowned jazz bassist Charles Mingus is airing nationally via public broadcasting television channels). It may also demand normative evaluations about the importance of particular categories of information (e.g., the search engine may have to choose in what order to rank information turned up in the name search about the search subject's current place of employment as opposed to a past criminal conviction). Within that context, a search engine's return of search results represents the sort of expression of opinion that scholars and lawyers such as Eugene Volokh and Donald Falk have noted warrants protection as speech under the U.S. First Amendment.³⁶

Even pre-Costeja, the complex nature of search engines, their interactions with users, and the impact of the results they deliver suggested to some that more nuanced global governance approaches to regulation (supplementing the sort of local regulation we might expect over relevant issues such as intellectual property, privacy, and speech) might be appropriate.³⁷ In the

or linking users to an online location containing infringing material or infringing activity" and including "a directory, index, reference, pointer, or hypertext link". The Canadian Copyright Act uses this term in a similar context to refer to "any tool that makes it possible to locate information that is available through the Internet or another digital network". R.S.C., 1985, c. C-42, § 41.27. As used herein, the term refers broadly to online applications and platforms that identify and link to third-party content in response to user queries.

- 35 Within these categories, one may be seeking information about ocean-faring striped bass or freshwater largemouth and smallmouth bass. Or, one may be seeking information about low-tuned stringed instrument. More specifically, one may want information about acoustic (upright) varieties of that instrument, or about electric bass guitars, or about the use of that instrument to accompany a violin, viola, and cello in a classical orchestra; a guitar and drums in a rock band; or a piano in the jazz setting. Drilling down further, one may want information at the level of music theory, information about purchasing an instrument, and/or information about well-known performers.
- 36 See Eugene Volokh and Donald Falk, "First Amendment Protection for Search Engine Search Results-White Paper Commissioned by Google", *UCLA School of Law Research Paper*, n.º 12-22 (2012), <http://dx.doi.org/10.2139/ssrn.2055364>.
- 37 See Urs Gasser, "Regulating Search Engines: Taking Stock and Looking Ahead", *Yale Journal of Law and Technology* 8, n.º 1 (2006): 234, <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1028&context=yjolt>

era of RTBF—and increasing trends of interventions that disrupt the flow of information among searcher, search engine, and search subject—these considerations are even more important.

C. Privatization of Governance Functions

The evolution of the Internet has been characterised by entanglement among public and private institutions. Vital and impactful decisions that implicate core human values like the right to free expression—classically, subjects of decision making via local institutions—are often delegated to non-public commercial entities. Such delegation and—more broadly—the establishment of close ties between private actors and public institutions raise significant questions concerning due process, individual freedoms, and user rights.³⁸

The implementation of RTBF post-Costeja has highlighted the complexities associated with a private company's controlling functions with such significant public impacts. Google complies by its obligations by: (a) fielding RTBF requests from individuals (who request that certain search results be removed from search); and (b) implementing and managing systems for evaluating and processing those requests relies largely on mechanisms internal to Google.³⁹ As more and more companies adopt RTBF frameworks, there will inevitably be increasing fragmentation along a number of axes:

[B]eyond the general directions provided by the ECJ in Google Spain, the RTBD as currently implemented is, in two respects, subject to a risk of fragmentation: first, due to the plurality of search engines bearing the task of directly implementing it, though Google's current pre-eminence in that market does well to hide this risk; second, due to the fact that, also at the DPA level, there are no commonly agreed-upon standards of RTBD claim management, though the current focus on Google as the main gatekeeper of the RTBD along with the lack of appeals to local DPAs, again, tends to overshadow the issue.⁴⁰

Non-public decision-making frameworks inherently lack transparency and carry the potential for abuse. And, private actors charged with implementing the right to be forgotten may

(noting that “[t]hree basic values—informational autonomy, diversity, and, information quality—intersect the policy debates surrounding the role and function of search engines within the digital environment” and that “these considerations may chart out a more comprehensive governance framework which effectively addresses total policy concerns, yet retains the flexibility to respond to technological change and innovation”.).

38 See Nicolas Arpagian, “The Delegation of Censorship to the Private Sector”, in *Turn to Infrastructure*, 164 (“The establishment of a strong, sustainable, and deep relationship between the private sector and the public administrations is likely bound to restrain individual freedoms—because a power can only be limited by another power”.). See also DeNardis, “The Global War”, 15 (“Questions about the privatisation of Internet governance are not only about freedom of expression but about economic liberty for private companies offering Internet services as well as for individuals relying on these private infrastructures”).

39 See Mark Scott, “Google Details Problems with Handling Right to Be Forgotten Requests”, *The New York Times*, July 31, 2014, <https://bits.blogs.nytimes.com/2014/07/31/google-details-problems-with-handling-right-to-be-forgotten-requests/>.

40 Reymond, “Square Pegs”, 10.

not be accountable to the full range of individuals implicated by their decisions. Overreliance on private companies in this context might lead to a perception that decisions about RTBF lack the level of legitimacy to which governance frameworks aspire, and that are especially important in highly charged and politicised arenas such as privacy and speech.⁴¹ Consideration of multi-stakeholder governance models in the context of RTBF might help to ameliorate these concerns.

D. Jurisdictional Considerations

Finally—and perhaps most importantly—a global Internet poses significant challenges for classic conceptions of jurisdiction, choice of law, and enforcement of judicial process relating to content. The idea that a nation should be able to legislate and regulate within its borders—consistent with its internal, shared national values and traditional principles of democratic governance—is put to the test on an ostensibly borderless web. Management of content takedown requests with cross-border implications demands that a delicate balance be struck among national and global interests.

RTBF highlights these challenges and serves, in some ways, as a perfect case study to address this tension between national sovereignty and global Internet access.⁴² In a widely-publicised case in France, for example, Google was asked by a French RTBF claimant to delist search results and complied by removing such results from its google.fr French site; then from other European sites (e.g., google.de and google.it); and ultimately from all Google sites—even non-European sites like google.com and google.ca—in search results displayed to European users. France’s data protection authority—the Commission Nationale de L’informatique et des Libertés (“CNIL”)—sought more, however, arguing that full implementation of the RTBF demanded removal of results from all Google regional platforms, for searchers in all countries around the world. CNIL’s arguments raised red flags for scholars and advocates of free expression around the world.⁴³

41 See Ryan Budish, Sarah Meyers West, and Urs Gasser, “Designing Successful Governance Groups: Lessons for Leaders from Real-World Examples” *Berkman Klein Center for Internet & Society, Research Publication*, n.º 2015-11 (2015): 5, 11, <http://dx.doi.org/10.2139/ssrn.2638006>. (Noting that “traditional sources of legitimacy” include “elections or constitutional authority” and that legitimacy is “more frequently called into question” in domains that—like RTBF—are “highly politicised”).

42 Giancarlo Frosio, “Right to Be Forgotten: Much Ado About Nothing”, *Colorado Technology Law Journal* 15, n.º 2 (2017): 329, <https://ssrn.com/abstract=2908993>. (“The extraterritorial application of the right to be forgotten remains perhaps the thorniest issue to be dealt with in its implementation”).

43 See, e.g., Bruce D. Brown, “News organizations must unite with tech world on ‘right to be forgotten’” *Reporters Committee for Freedom of the Press*, May 19, 2016, <https://www.rcfp.org/browse-media-law-resources/news/news-organizations-must-unite-tech-world-right-be-forgotten>; Daphne Keller, “Global Right to Be Forgotten Delisting: Why CNIL is Wrong”, *The Center for Internet and Society (blog)*, November 18, 2016, <http://cyberlaw.stanford.edu/blog/2016/11/global-right-be-forgotten-delisting-why-cnil-wrong>; Nani Jansen Reventlow, Vivek Krishnamurthy and Christopher T. Bavit, “A French court case against Google could threaten global speech rights”, *The Washington Post*, December 22, 2016, https://www.washingtonpost.com/news/global-opinions/wp/2016/12/22/a-french-court-case-against-google-could-threaten-global-speech-rights/?utm_term=.001a3a5056d6.

Two recent non-RTBF cases underscore the ways in which these types of cross-border disputes over content takedowns can play out. First, in *Google LLC v. Equustek Solutions Inc.*, Case No. 5:17-cv-04207-EJ, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017), the Supreme Court of Canada addressed the fashioning of remedies in a trade secret and trademark dispute between two private companies: Canadian tech firm, Equustek, and its former distributor, Datalink. That underlying dispute resulted in an order to Google (not a party to the underlying dispute) to delist from search specific web pages associated with Datalink and its sale of unauthorised computer hardware. Google deindexed pages on its Canadian, google.ca, search engine. The Supreme Court held that this was inadequate, rejecting Google's arguments about comity and territoriality, and ordered Google to undertake delisting worldwide. Google ultimately sought relief from that order in the US, obtaining a preliminary injunction against enforcement of the order in a United States federal district court.⁴⁴

Second, in *Spanski Enterprises, Inc. v. Telewizja Polska, S.A.*, n.º 17-7051 (D.C. Cir. 2018), the United States Court of Appeals for the District of Columbia Circuit examined claims brought against an ex-US website that directed content into the United States in violation of plaintiff's exclusive US public performance rights. In holding the defendant liable, the Court strongly suggested that foreign websites should geoblock content —i.e., determine the location of users attempting to access that content and grant or deny access based on applicable local law—in order to avoid local copyright liability for cross-border content transmissions.⁴⁵

On the one hand, the *Spanski* case demonstrates that local courts have the ability to adjudicate technical issues on given facts that relate to cross-border content disputes. And, the *Equustek* cases demonstrate that courts have the ability to fashion remedies deemed appropriate in the context of local laws and norms (see, e.g., the actions of the Canadian Supreme Court) and to cabin remedies implemented by foreign courts when they impinge upon rights and freedoms under local law (see, e.g., the actions of the United States District Court). But, these types of case-by-case adjudications are complex and resource intensive. They may lead to inconsistent outcomes that complicate matters for both users and service providers operating in different countries. And, they are unlikely to lead to full and balanced vindication of the rights of all parties implicated (or aggrieved) by content determinations worldwide. This is particularly true with an issue —like RTBF— that impacts core functions of information location online.

E. Drawing on Internet Governance Frameworks in Addressing the RTBF

Given these characteristics of the right to be forgotten, approaches to RTBF that draw on Internet governance frameworks —and, in particular, multi-stakeholder engagement involving both public and private actors— might help to ensure that just outcomes are achieved via fair transparent processes that balance global and local interests. In particular:

44 *Google LLC v. Equustek Solutions Inc.*, Case n.º 5:17-cv-04207-EJ, 2017 WL 5000834 (N.D. Cal. November 2, 2017).

45 *Spanski Enterprises, Inc. v. Telewizja Polska, S.A.*, n.º 17-7051 (D.C. Cir. 2018); see Marketa Trimble, "D.C. Circuit Makes Geoblocking De Facto Mandatory for Copyright Law Purposes-Spanski v. TV Polska", *Technology & Marketing Law Blog (blog)*, March 8, 2018, <https://blog.ericgoldman.org/archives/2018/03/d-c-circuit-makes-geoblocking-de-facto-mandatory-for-copyright-law-purposes-spanski-v-tv-polska-guest-blog-post.htm>.

- *Decisionmakers should draw upon history, scholarship, and long-standing experience of legacy IG institutions.* At its heart, RTBF raises fundamental questions about the identification and dissemination of information. Institutions involved in Internet governance have decades of experience addressing considerations relevant to IG in the context of RTBF. Those institutions, in turn, have drawn upon decades of prior experience with governance considerations involving a wide range of pre-Internet technological innovations.⁴⁶ Jeremy Malcolm of the Electronic Frontier Foundation has noted that existing Internet governance fora are imperfect but will “always be part of the global governance ecosystem”.⁴⁷ Decisionmakers can draw on the experience of long-standing institutions while simultaneously working to ensure they are “inclusive, balanced, and accountable”.⁴⁸
- *Decisionmakers should consider active, on-going multi-stakeholder efforts and frameworks that seek to reconcile speech and privacy concerns across jurisdictions.* The work of an institution such as the Internet & Jurisdiction Policy Network (“I&JPN”) may provide guidance on addressing, in particular, the cross-border impacts of RTBF. I&JPN is a Paris-based Secretariat that “facilitates a global multistakeholder process to enable transnational cooperation” in an effort to “preserve the cross-border nature of the Internet, protect human rights, fight abuses, and enable the global digital economy”.⁴⁹ Multi-stakeholder initiatives like I&JPN’s Content and Jurisdiction Workplan may provide a useful framework.⁵⁰ The work of colleagues at Harvard Law School’s Cyberlaw Clinic, released as a report entitled “Here, There, or Everywhere? Assessing the Geographic Scope of Content Takedown Orders”, attempts to establish a global framework for content takedown notices across jurisdictions, identifying categories of content takedowns that may warrant consistent treatment across national borders.⁵¹
- *Decisionmakers should coordinate across contemporaneous domains that raise similar emerging issues.* Finally, it is worth looking beyond the right to be forgotten —and the speech, privacy, and jurisdictional issues implicated thereby—to consider on-going governance discussions in other domains that raise similarly challenging concerns. For

46 See, e.g., Stefan Bechtold, “Governance in Namespaces”, *Loyola Law Review* 36, n.º 3 (2002): 1242, <https://digitalcommons.lmu.edu/llr/vol36/iss3/6/> (addressing governance in Internet namespaces by reference to “[t]elephone numbers, Social Security numbers, the International Standard Book Number (ISBN), zip codes, bar codes, and bibliographic classification schemes”, all of which “form namespaces too”).

47 Jeremy Malcolm, “Is Multi-Stakeholder Internet Governance Dying”, *Electronic Frontier Foundation, Deeplinks (blog)*, December 20, 2017, www.eff.org/deeplinks/2017/12/multi-stakeholder-internet-governance-dying.

48 Malcolm, “Is Multi-Stakeholder Internet Governance Dying”.

49 Internet & Jurisdiction Policy Network, <https://www.internetjurisdiction.net/about/mission> (describing the work of the Paris-based Secretariat).

50 See <https://www.internetjurisdiction.net/work/content-jurisdiction>.

51 Alicia Solow-Niederman, Francisco Javier Careaga Franco, Nani Jansen Reventlow, and Vivek Krishnamurthy. 2017. *Here, There, or Everywhere? Assessing the Geographic Scope of Content Takedown Orders*. Working Paper, Cyberlaw Clinic, Harvard Law School, March 27, <http://clinic.cyber.harvard.edu/files/2017/03/Here-There-or-Everywhere-2017-03-27.pdf>.

example, contemporaneous with the evolution of RTBF, questions about governance and regulation of secure encryption technologies offered by private companies to private citizens represent another emerging and equally useful case study. As with search, the field of encryption is one that is technical and one in which “domestically and internally oriented” policy determinations can have massive global “ripple effects”.⁵² As parallel debates play out around RTBF and encryption —in terms of establishing legitimate oversight mechanisms and mitigating damaging cross-border effects that improperly impinge on national sovereignty— those pursuing governance in each of these arenas might draw on the experiences of the other.

CONCLUSION

The development and proliferation of right to be forgotten frameworks around the world raise issues that are neither new nor unique to RTBF. But, as particular implementations of RTBF blur lines between infrastructure and content, such regimes serve to underscore the interconnected roles played by a wide range of stakeholders in the Internet ecosystem and the complexities involved in addressing the needs of those stakeholders. Coordination among local and international, public and private, individual and institutional, in decisions that have global impacts on users’ ability to access information online is vital.

It is neither reasonable nor appropriate to expect consistency across jurisdictions regarding the substance of content regulation and the highly charged speech and privacy considerations implicated thereby. But, integration of global governance frameworks into decision making about topics that —like RTBF— straddle lines, can ensure some degree of interoperability, legitimacy, respect for the role of local and national decision making, and recognition of shared values.

BIBLIOGRAPHY

Jurisprudence, legalization, and policies

1. Belgian Supreme Court. P.H. v. O.G. ref. C.15.0052.F. (Abril 29, 2016).
2. Corte Constitucional de Colombia. Sentencia T-277/15 (M.P. María Victoria Calle Correa: May 12, 2015).
3. Court of Justice of the European Union. (Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González). C-131/12 (May 13, 2014).

52 See Ryan Budish, Herbert Burkert, and Urs Gasser. 2018. Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects. Aegis Series Paper n.º 1804, Hoover Institution Essay, March 2, https://www.hoover.org/sites/default/files/research/docs/budish_webreadypdf.pdf.

4. European Parliament and of the Council. "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". Official Journal 2016/679. Art. 94. April 27, 2016.
5. European Union. "Directive 95/46". Official Journal L 281/31. November 23, 1995.
6. Google LLC v. Equustek Solutions Inc. Case n.º 5:17-cv-04207-EJ, 2017 WL 5000834 (N.D. Cal. November 2, 2017).
7. International Organisation for Standardisation. *Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model* (ISO/IEC 7498-1, 2.^a Ed., 1994-11-14, corrected and reprinted 1996-06-15): 32-52. [http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994\(E\).zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip).
8. Spanski Enterprises, Inc. v. Telewizja Polska, S.A., n.º 17-7051 (D.C. Cir. 2018).

Articles

9. Akshabi, Saamer and Constantine Dovrolis. "The Evolution of Layered Protocol Stacks Leads to an Hourglass-Shaped Architecture (extended version)". *Georgia Tech College of Computing*, <https://www.cc.gatech.edu/~dovrolis/Papers/evoarch-extended.pdf>.
10. Bechtold, Stefan. "Governance in Namespaces". *Loyola Law Review* 36, n.º 3 (2002): 1242, <https://digitalcommons.lmu.edu/llr/vol36/iss3/6/>.
11. Beck, Micah. "On the Hourglass Model". *Arxiv.org*. (2015), <https://arxiv.org/abs/1607.07183>.
12. Budish, Ryan, Sarah Meyers West, and Urs Gasser. "Designing Successful Governance Groups: Lessons for Leaders from Real-World Examples". *Berkman Klein Center for Internet & Society, Research Publication*, n.º 2015-11 (2015): 5, 11, <http://dx.doi.org/10.2139/ssrn.2638006>.
13. Budish, Ryan, Herbert Burkert and Urs Gasser. "Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects". *Hoover Institution Essay*, n.º 1804 (2018), https://www.hoover.org/sites/default/files/research/docs/budish_wbready.pdf.
14. Committee on the Internet in the Evolving Information Infrastructure, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, *The Internet's Coming of Age* (Washington, D. C.: National Academy Press 2001), 36.
15. Gasser, Urs. "Regulating Search Engines: Taking Stock and Looking Ahead". *Yale Journal of Law and Technology* 8, n.º 1 (2006): 234, <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1028&context=yjolt>.
16. Frosio, Giancarlo. "Right to Be Forgotten: Much Ado About Nothing". *Colorado Technology Law Journal* 15, n.º 2 (2017): 329, <https://ssrn.com/abstract=2908993>.
17. Heverly, Robert A. "Breaking the Internet: International Efforts to Play the Middle against the Ends: A Way Forward". *Georgetown Journal of International Law* 42, n.º 4 (2011): 1090, <https://ssrn.com/abstract=1825304>.

18. Keller, Daphne. "The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation". *Stanford Law School Center for Internet and Society*, (2017): 35, <http://dx.doi.org/10.2139/ssrn.2914684>.
19. Kelly, Michael J. and David Satola, "The Right to be forgotten". *University of Illinois Law Review* 2017, n.º 1 (2017): 3, <https://illinoislawreview.org/print/volume-2017-issue-1/the-right-to-be-forgotten/>.
20. Perry Barlow, John. "A Declaration of the Independence of Cyberspace". *Electronic Frontier Foundation*. (1996), <https://www.eff.org/cyberspace-independence>.
21. Reymond, Michel J. "Hammering Square Pegs into Round Holes: The Geographical Scope of Application of the EU Right to be delisted". *Berkman Klein Center for Internet & Society, Research Publication*, n.º 2016-12 (2016): 1, <http://dx.doi.org/10.2139/ssrn.2838872>.
22. Solow-Niederman, Alicia, Francisco Javier Careaga Franco, Nani Jansen Reventlow, and Vi-
vek Krishnamurthy. "Here, There, or Everywhere? Assessing the Geographic Scope of Content Takedown Orders. *Cyberlaw Clinic, Harvard Law School* (2017), <http://clinic.cyber.harvard.edu/files/2017/03/Here-There-or-Everywhere-2017-03-27.pdf>.
23. Volokh, Eugene and Donald Falk. "First Amendment Protection for Search Engine Search Results-White Paper Commissioned by Google". *UCLA School of Law Research Paper*, n.º 12-22 (2012), <http://dx.doi.org/10.2139/ssrn.2055364>.

Doctrine

24. Arpagian, Nicolás. "The Delegation of Censorship to the Private Sector". In *Turn to Infrastructure in Internet Governance*. Eds., Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, Nanette S. Levinson, 164. US: Palgrave Macmillan US, 2016.
25. Bygrave, Lee A., Susan Schiavetta, Hilde Thunem, Annebeth B. Lange, and Edward Phillips. "The naming game: governance of the Domain Name System". In *Infrastructure and Institutions*, eds., Lee A. Bygrave y Jon Bing, 147. New York: Oxford University Press, 2009.
26. Bygrave, Lee A. and Terje Michaelsen. "Governors of Internet". In *Infrastructure and Institutions*, eds., Lee A. Bygrave y Jon Bing, 115. New York: Oxford University Press, 2009.
27. DeNardis, Laura. *The Global War for Internet Governance*. New Haven: Yale University Press, 2014, 20.
28. DeNardis, Laura and Francesca Musiani. "Governance by Infrastructure". In *The Turn to Infrastructure in Internet Governance*, eds., Francesca Musiani, Derrick L. Cogburn, Laura De-
Nardis, and Nanette S. Levinson, 4, Palgrave Macmillan, 2016.
29. de Terwangne, Cécile. "The Right to be Forgotten and Informational Autonomy in the Digital Environment". In *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten*, eds., Ângela Pereira, Alessia Ghezzi, and Lucia Vesnic-Alujevic, 83-84. Palgrave MacMillan, 2014.
30. Solum, Lawrence B. "Models of Internet governance". In *Internet Governance: Infrastructure and Institutions*, eds., Lee A. Bygrave and Jon Bing, 50. U.K.: Oxford University Press, 2009.

31. van der Spuy, Anri. *What if we all governed the Internet? Advancing multistakeholder participation in Internet governance*. Unesco Publishing, 2017, 25.
32. Zittrain, Jonathan. *The Future of the Internet and How to Stop It*, 68, fig. 4.1. New Haven: Yale University Press, 2009.

The media, blogs, and Web Pages

33. Brown, Bruce D. "News organizations must unite with tech world on 'right to be forgotten'". *Reporters Committee for Freedom of the Press*, May 19, 2016, <https://www.rcfp.org/browse-media-law-resources/news/news-organizations-must-unite-tech-world-right-be-forgotten>.
34. Deering, Steve. Watching the Waist of the Protocol Hourglass (Londres: IETF 51, August, 2001), <https://www.iab.org/wp-content/IAB-uploads/2011/03/hourglass-london-ietf.pdf>.
35. Keller, Daphne. "Global Right to Be Forgotten Delisting: Why CNIL is wrong". *The Center for Internet and Society (blog)*, November 18, 2016, <http://cyberlaw.stanford.edu/blog/2016/11/global-right-be-forgotten-delisting-why-cnil-wrong>.
36. Kleinwächter, Wolfgang. Towards a Holistic Approach for Internet Related Public Policy Making. *Global Commission on the Stability of Cyberspace Thought Piece*, 2018, 7-8, <https://cyberstability.org/research/thought-piece-towards-a-holistic-approach-for-internet-related-public-policy-making/>.
37. Malcolm, Jeremy. "Is Multi-Stakeholder Internet Governance Dying". *Electronic Frontier Foundation, Deeplinks (blog)*, December 20, 2017, <https://www.eff.org/deeplinks/2017/12/multi-stakeholder-internet-governance-dying>.
38. Reventlow, Nani Jansen, Vivek Krishnamurthy and Christopher T. Bavitz. "A French court case against Google could threaten global speech rights". *The Washington Post*, December 22, 2016, https://www.washingtonpost.com/news/global-opinions/wp/2016/12/22/a-french-court-case-against-google-could-threaten-global-speech-rights/?utm_term=.001a3a5056d6.
39. Scott, Mark. "Google Details Problems with Handling Right to Be Forgotten Requests". *The New York Times*, July 31, 2014, <https://bits.blogs.nytimes.com/2014/07/31/google-details-problems-with-handling-right-to-be-forgotten-requests/>.
40. Trimble, Marketa. "D.C. Circuit Makes Geoblocking De Facto Mandatory for Copyright Law Purposes-Spanski v. TV Polska". *Technology & Marketing Law Blog (blog)*, March 8, 2018, <https://blog.ericgoldman.org/archives/2018/03/d-c-circuit-makes-geoblocking-de-facto-mandatory-for-copyright-law-purposes-spanski-v-tv-polska-guest-blog-post.htm>.
41. Zittrain, Jonathan. "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>.