SPEECH ACROSS BORDERS

BY JENNIFER DASKAL


ABSTRACT

As both governments and tech companies seek to regulate speech online, these efforts raise critical, and contested, questions about how far those regulations can and should extend. Is it enough to take down or delink material in a geographically segmented way? Or can and should tech companies be ordered to takedown or delink unsavory content across their entire platforms—no matter who is posting the material or where the unwanted content is viewed? How do we deal with conflicting speech norms across borders? And how do we protect against the most censor-prone nation effectively setting global speech rules? The questions were recently addressed in two high-profile judgments from the European Court of Justice and were the subject of ongoing litigation that pitted Canadian and U.S. courts against one another. Meanwhile, a new form of geographically-segmented speech regulation is emerging—pursuant to which speech is limited based on who is speaking and from where, as opposed to what is being said.

This Article examines the ways in which norms regarding speech, privacy, and a range of other rights conflict across borders, the power of private sector players in adjudicating and resolving these conflicts, the ways in which governments are seeking to harness this power on a global scale, and the broader implications for individual rights. It offers a nuanced approach that identifies the multiple competing interests at stake—recognizing both the ways in which global takedowns or delinkings can, at times, be a critical means of protecting key interests, and the risk of over-censorship and forced uniformity that can result.

TABLE OF CONTENTS

INTRODUCTION........................................................................................................................................ 2

I. THE STATE OF PLAY: CONTENT TAKE DOWN ORDERS WITH GLOBAL REACH? ................................................................. 10

---

* Jennifer Daskal is an Associate Professor at American University Washington College of Law. Special thanks to Kevin Benish, Danielle Citron, Julie Cohen, Jean Galbraith, Daphne Keller, Kate Klonick, Neil Richards, Paul Schwartz, Peter Swire, participants at Georgetown’s 2019 Tech Law & Policy Colloquium, Vanderbilt Law’s September 2019 Faculty Law Workshop, the 2018 Amsterdam Privacy Conference, the 2018 Privacy Law Scholars Conference, the 2018 International Law in Domestic Court Workshop at University of Pennsylvania Law School, and Temple Law School’s International Law Colloquium, my incredibly helpful research assistants Daniel de Zayas and Sara Shaw, and my American University Washington College of Law colleagues for helpful input, conversations, and thoughts.
INTRODUCTION

In the waning days of summer 2019, Hong Kong police clashed regularly and often violently with protesters who, among other things, demanded greater independence from China. For a while, China watched in what appeared to be silence. But numerous social media accounts started popping up on Facebook, Twitter and elsewhere—decrying the protesters as “cockroaches” acting at the behest of Western forces.¹ Social media companies concluded that many of these accounts were fake, created by Chinese government agents and officials to discredit the protesters. In response, Facebook shut down five accounts, seven pages, and three Facebook groups; Twitter suspended close to 1,000 active accounts.² Three

---


days later, Google reported that it had barred 210 channels on YouTube for the same reasons. China condemned the actions, echoing the critiques of others who have denounced U.S. social media companies as global censors.

The clash between China and the tech companies is one of many struggles to control speech across borders—a struggle that is pitting governments against one another and private actors against public ones. This Article examines these conflicts through the lens of four major court cases—cases that raise critically important questions about the geographic reach of and nature of speech regulations—as well as a discussion of private sector decision making in response. In each of these cases, courts have sought to impose speech regulations globally, across entire platforms, in ways that require private companies to delink, take down, and in some cases monitor for and keep off unwanted speech, regardless of where the speaker or listener is located. And in each of these cases, private companies have resisted, arguing that even if they can be compelled to take unwanted speech offline locally, so that users in a particular jurisdiction cannot access it, they should not be required to delink or take down the unwanted speech outside that jurisdiction demanding it. The cases themselves cover a range of different kinds of content and range of different kinds of orders, ranging from simple delinking orders to broad obligations to monitor for and keep off unwanted speech online.

The broadest—and most troubling of the four—derives from an April 2016 Facebook post, in which a user shared an article about and photo of Ms. Eva Glawischnig-Piesczek, then-chair of the Green Party, along with commentary labeling her a “lousy traitor,” “corrupt oaf,” and member of a “fascist party.” Ms. Glawischnig-Piesczek asserted that she had been
defamed and, with the backing of an Austrian court, demanded that Facebook delete the post. The court further demanded that Facebook monitor for copycat posts and remove those as well. Facebook took down the specific, identified post, but objected to the ongoing monitoring and takedown obligations. And it took down the particular post in a geographically segmented way only. As a result, the post was inaccessible to anyone who logged onto Facebook in Austria; it, however, could potentially be accessed elsewhere. The parties appealed, all the way to the Austrian Supreme Court.

The Austrian Supreme Court affirmed the finding of defamation, then referred the case to the European Court of Justice (“CJEU”) to identify the permissible scope and geographic reach of the order. Specifically, the Austrian Court asked the CJEU to consider whether Facebook could, in addition to being required to take down the specific post at issue, be ordered to identify and delete “identically worded” and “equivalent” attacks on the Green party leader as well. The court also asked whether any such takedown requirements could be imposed on a worldwide basis, or whether Austrian courts could require monitoring and blocking in Austria only.

In an October 2019 ruling, the European Court gave the Austrian court the green light that Ms. Glawischnig-Piesczek wanted -- concluding that nothing in EU law precludes takedown and monitoring orders of global reach. Per the European Court’s ruling, the Austrian court could, and very well may, tell Facebook that they have to both take down the offending post and prevent anyone, anywhere around the world, from posting an equivalent one as well. The first part—dealing with the specific, identified post—is not particularly surprising. As the Court conclude, the geographic reach of such
orders is a matter of national and public international, not EU, law. But the Court’s additional conclusion that member states could impose additional monitoring obligations—to look for and take down “equivalent” conduct and do so around the world—seems to fly in the face of other EU law rules which prohibit courts from imposing general monitoring obligations on private providers. And it raises the specter of national courts acting as global censors and enlisting private companies as minions on their behalf.

The case now goes back to the Australia courts, which will have to decide whether and how broadly to impose any such monitoring requirements. National courts throughout the EU, and elsewhere, now also have the go-ahead to issue similar orders with broad reach and will, as a result, have to struggle with the critically important questions as to whether and when such kinds of global monitoring requirements are legitimate.

In another widely-watched case, issued just a week before the Austrian case, France demanded that Google implement the so-called right to be forgotten—now codified in the EU’s General Data Protection Regulation (“GDPR”) as the “[r]ight to erasure”—globally. Pursuant to the right to be forgotten, individuals can demand that search engines delink from the search of their name articles or information that is deemed embarrassing or no longer relevant, even if true. Google had agreed to delink the unwanted information for anyone searching the individual’s name from Europe but had left it accessible for searches originating outside Europe. This time, the European Court sided with Google, concluding that EU law does not provide a basis for mandating delinkings with global reach. Yet, it did so in a way that, consistent with the Austria Facebook decision, left open the possibility national courts could, under their domestic

16 Judgment Facebook Opinion, Pars. 48-52.
17 Id. Par. 46-47; see also Council Directive 2000/31, art. 15(1), 2000 O.J. (L 178) 13; infra Part II.B.
18 See Daskal, A European Court Decision May Usher in Global Censorship, supra note 20.
21 See, e.g. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) (Google Spain Case), 2014 ECLI:EU:C:2014:317 ¶¶ 91-96 (providing guidance regarding the parameters and implementation of the right to be forgotten).
22 Judgment, Google v. CNIL, C 507/17, ¶¶ 31-32 (describing Google’s responses to France’s demands).
23 Id. ¶ 64.
law do just that—require delinking across the entire platform, regardless of where the information originated from or was accessed.  

Analogous—although in key ways different—conflicts over the scope of speech online have been playing out in cross-border disputes involving Australian, Canadian, and U.S. courts. In September 2017, the Supreme Court of New South Wales ordered Twitter to take down accounts that were distributing confidential financial information about the plaintiff and to prevent the offenders from opening and operating new accounts. The Court imposed this obligation across all of Twitter, anywhere Twitter operates around the world. The Canadian Supreme Court similarly demanded that Google engage in a global take down of particular websites in an attempt to protect against an alleged intellectual property violation.

In each of these cases, courts and national governments have sought to impose global delinking and takedown orders and private companies have fought to keep content up rather than taking it down—taking the converse position of that adopted with respect to the Chinese-supported social media accounts. Each raise critically important questions about the appropriate nature and scope of speech regulations, the prospect of harmonization (or not) across borders, the interplay between speech, privacy, economic and a myriad of other rights, and the dynamic relationship between governments, courts, and companies in setting the rules. In these cases, it is the companies, and their supporters, that are rallying against global censorship—arguing that no one country or court should be able to impose its particular content regulations across the globe.

Yet, as the Chinese government complained about when Twitter, Google, and Facebook took down the anti-Hong Kong protester commentary, companies do just that all the time, set global speech policies and practices via terms of service and community standards that apply universally on their platforms across all the jurisdictions in which they operate. Facebook’s Community Standards, for example, which dictate what is and is not permitted on the platform, "apply to everyone, all around the world."

---


26 Id. Twitter objected to the jurisdiction of the court. It did not actually appear before the court, but instead submitted an anonymous email that laid out key objections. Id. ¶¶ 3, 23.


the world, and to all types of content.”29 Other large multinational tech companies similarly employ content policies and codes of conduct globally and across numerous different issue-areas—in response to alleged copyright infringements, concerns over terrorist use of the Internet, child pornography, bullying, hate speech, and nudity online, among many other areas.

We have, as described by Professor Jack Balkin, entered a new speech paradigm—one that is “pluralist rather than dyadic,” in which online platforms have the power to disseminate and control speech both domestically and across territorial borders.30 Professor Kate Klonick has similarly detailed the ways in which these “New Governors” control the scope and nature of speech online.31 Moreover, the effect is on much more than just speech. Decisions about what is and is not permitted online have implications for privacy, security, and a range of other rights and interests as well. The effect of these decisions are often unlimited by territorial boundaries.32

---

31 See Kate Klonick, The New Governors: The People, Rules, and Processes Governing Online Speech, 131 Harv. L. Rev. 1598, 1603 (2018) (describing tech companies “as the New Governors of online speech” and thus “part of a new triadic model of speech that sits between the state and speakers-publishers”); see also Jennifer Daskal, Borders and Bits, 71 Vand. L. Rev. 179, 181 (2018) (discussing the role “of private, third-party providers in setting the rules” governing internet use); Alan Z. Rozenshtein, Surveillance Intermediaries, 70 Stan. L. Rev. 99, 99 (2018) (analyzing the role of tech companies as “surveillance intermediaries”); Balkin, Free Speech in the Algorithmic Society, supra note 30, at 1187–88 (discussing the role of companies like Facebook in governing “digital expression”); Kristen E. Eichensehr, Digital Switzerlands, 167 U. Pa. L. Rev. 665, 672 (2019) (more generally describing the ways in which “major U.S. technology companies have grown into power centers that compete with territorial governments”). A similar point can be made about security and the changing nature of criminal investigations and evidence gathering. What used to involve a relationship between territorial governments, law enforcement entities, and their citizenry is now being mediated by multinational, private tech companies that are served requests for data and determine whether and how to comply—often with little to no visibility to the end user. See Jennifer Daskal, The Opening Salvo: The CLOUD Act, e-Evidence Proposals, and EU-US Discussions Regarding Law Enforcement Access to Data Across Borders (book chapter, forthcoming 2019).
32 See Daskal, Borders and Bits, supra note 31, at 182 (noting the ways in which “[t]he multinational companies that manage our data have taken on a form of international governance in ways that traditional governments can’t and won’t”).
The small number of court cases highlighted in the first part of this Article are thus exemplary—the tip of the iceberg with respect to takedown and delinking determinations being made on a daily basis. Private tech companies also are routinely deciding exactly the issues presented by these cases—whether particular content should be accessible or deleted, whether and in what circumstances local speech restrictions should be applied locally or globally, and how to set the boundaries of any applicable restrictions. Yet, because the four highlighted cases are public and court-ordered, they are critically important—setting baseline rules against which the companies operate and setting the standards for future cases and controversies. Together, they case illuminate four key issues.

First, governments and private parties now recognize and seek to harness the power of the private sector in controlling the dissemination of information and ideas, not just locally but globally. The court cases are a public, transparent reflection of that. But these are just one mechanism by which governments and private actors seek to influence speech norms online. Both governments and private actors also spend significant energy convincing, coercing, or cajoling companies to curate or disseminate content in less transparent matters, even in the absence of direct legal or regulatory requirements to do so.

Second, and relatedly, any effort to curate content online—whether mandated or voluntary—raises critically important questions about geographic reach. After all, control over online platforms has the potential to result in control over global communications, not just local speech. Conversely, both governments and platforms have the option of responding to divergent speech norms in geographically segmented ways.

Third, curation of content implicates a broad spectrum of interests, rights, and values, beyond the obvious speech implications. The right to be forgotten case highlights a potential clash between free speech and privacy interests, including the interest in controlling what personal information is shared and disseminated online. The Canadian Google case pits speech

---

33 The small subset of cases that in fact make it to the courts arise only if there is a particular confluence of situations: (i) a government or judge orders a company to take down or delink content; (ii) the takedown or delinking order conflicts with a speech norm or interest that the tech company thinks is worth fighting for; (iii) a locally-implemented takedown or delinking order is deemed insufficient to satisfy the interest underlying the order.


35 See Judgment, Google v. CNIL Par. 60, 63, 67, 72 (describing right to be forgotten as balanced against the right to receive information, and recognizing that even in the EU nations differ in how they strike the appropriate balance); Whitney v. California, 274 U.S. 357, 375 (1927) (Brandeis, J., concurring) (The “freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth; . . . without free speech and assembly discussion would be futile . . . .”);
against intellectual property interests. The Austrian defamation case, by contrast, restricts what is in effect political, albeit inflammatory, commentary, thus running headlong into the core understanding of free speech as critical to the protection of a fair and open political process—one that is arguably a foundational component of a thriving, open democracy. Commentary that treats all such takedown and delinking orders as more or less equivalent intrusions on free speech misses this nuance.

* * *

The remainder of the Article delves into these issues as they are playing out in the courts and in company’s own policy-making. First, I explore in more detail the high-profile court cases in which governments have sought to set global speech norms and companies have resisted. Second, I look at a range of voluntary decisions to restrict content online by U.S.-based technology companies that often operate under the radar—via terms of service and a range of other internal decisions—and the geographic reach of these decisions. Third, I briefly highlight a new form of geographic
filtering elucidated by recent efforts to limit speech based on the location of the speaker, rather than the location of the listener—issues that have arisen in connection with efforts to control foreign influence in local elections. I conclude by addressing the normative questions. When and how should governments insist that takedowns or delinkings be done globally and when in a geographically segmented manner? What are the relevant interests at stake? How should they be accommodated across borders? In identifying the key considerations and possible responses, I propose specific, concrete ways to think through and ideally resolve the conflicts that emerge. In so doing, I also address the need for new accountability and transparency mechanisms that account for the shifting power sources—namely the private companies that operate across borders and do not rely on the voting booth for support.

I. THE STATE OF PLAY: CONTENT TAKE DOWN ORDERS WITH GLOBAL REACH?

The geographic scope of contested content takedown have played out in the European Court of Justice in two separate cases: one with respect to the European Union’s right to be forgotten and another with respect to a potentially far-reaching Austrian defamation ruling. In both cases, the governments—France and Austria, respectively—sought global takedown orders, whereas the affected companies agreed to block or delink the relevant content if accessed from all or parts of the EU, but refused to do so globally. Separate showdowns involving Twitter and Australia, in one case, and Google, the United States, and Canada, in another, raised geographic scope questions with respect to an alleged privacy intrusion claim and alleged trademark and trade secrets violation, respectively. Together, these cases highlight the complexity of the kinds of content-moderation issues that arise—exemplifying a range of different interests at stake and kinds of content-based restrictions that could be imposed.

These are the modern renditions of the 1990s dispute between France and Yahoo! over its auction site for Nazi memorabilia. But whereas in that early Internet case, France urged Yahoo! to segment the market and restrict access for those within France, governments, private parties, and some courts are now arguing that such geographic segmentation is insufficient. According to this view, takedowns and delinkings must be implemented globally to protect adequately the rights and interests at stake. The following delves into the detail of each of the four more recent cases, comparing them as well to the earlier Yahoo! case, thereby elucidating the deep complexity, along with the unique interests, considerations, and concerns that each raise.

https://searchenginewatch.com/2018/05/21/no-need-for-google-12-alternative-search-engines-in-2018/.
A.  **Google Spain Case and the Right To Be Forgotten: Back Before the CJEU**

In 2014, the European Court of Justice issued its opinion in the *Google Spain* case, affirming a far-reaching “right to be forgotten.” The case dates to 2010, when Mr. Costeja González, a Spanish national, demanded that Google remove links to then-sixteen-year-old newspaper articles that appeared when one typed Mr. Costeja’s name into Google and announced the auctioning of his repossessed home. Mr. Costeja never contested the article’s truthfulness. But he asserted that the underlying debts had been resolved, that the information was therefore no longer relevant, and that he had a right to control the disclosure of his personal information.

Google refused to delist the articles and the case ultimately made its way to the CJEU. The CJEU sided with Mr. Costeja. Relying on the then-applicable Data Protection Directive, it ruled that Google, as a search engine, was required to delist information associated with a search of Mr. Costeja’s name that is “inadequate, irrelevant or excessive in relation to the purposes of the processing . . . not kept up to date, or . . . kept for longer than is necessary unless . . . required to be kept for historical, statistical or scientific purposes”—even if the information is accurate. It further concluded that the right applies regardless of whether the data subject could show any prejudice.

In announcing this right, the CJEU acknowledged a potentially countervailing interest in information being made publicly available. Yet, it concluded that “as a general rule” the “data subject’s rights . . . override” the interests of other Internet users in accessing information. This “general rule” is modified if the data subject is a “public figure.” When dealing with
a public figure, the right must give way if there is a “preponderant interest of the general public in having . . . access to the information in question.”

The court did not define who constitutes a “public figure” or what constitutes a “preponderant interest” of the general public in the information.

Importantly, the CJEU placed the obligation to delist on Google, even though the newspaper that initially published the information could continue to make it available on its own website. According to the CJEU, there is something unique—and potentially privacy destructive—about the “ubiquitous” information available on a search engine. It thus shifted its regulatory focus away from the initial speaker (in this case, the newspaper that produced the content) toward the disseminator of the information (namely, the platforms and search engines that spread the information online). In so doing, it endorsed, amplified, and further entrenched the private sector’s power—and accompanying responsibility—in determining the scope of available content online.


45 Id. ¶ 16 (noting that the lower court allowed the La Vanguardia, the daily newspaper which published the articles, to keep the articles accessible on its website; that part of the opinion was not appealed to the CJEU). Since then, however, several courts have ordered newspapers to take down or anonymize articles that were the subject of right to be forgotten petitions. See, e.g., Brett Allan King, Spain High Court Issues First Right to Forget Ruling (2015), Bloomberg L., https://www.bna.co/spain-high-court-n57982062815 (discussing a similar decision in the highest court of Spain); Sebastian Schweda, Germany, Hamburg Court of Appeal Obliges Press Archive Operator to Prevent Name Search in Archived Articles, 1 Eur. Data Protection L. Rev. 299, 299–300 (2015) (discussing a German case ordering a newspaper to make articles potentially harmful to an individual’s reputation inaccessible online); Kristof Van Quathem, Right to be Forgotten—High Courts Disagree, Covington & Burling LLP: Inside Privacy (June 2, 2016), https://www.insideprivacy.com/international/european-union/right-to-be-forgotten-high-courts-disagree (discussing a case in which Belgium’s highest court held that individual privacy interest outweighed the public interest in accessing a decades-old article about a deadly accident involving a physician under the influence); Guido Scorza, A Ruling by the Italian Supreme Court: News Do “Expire”. Online Archives Would Need to Be Deleted, L’Espresso (July 1, 2016), http://espresso.repubblica.it/attualita/2016/07/01/news/a-ruling-by-the-italian-supreme-court-news-do-expire-online-archives-would-need-to-be-deleted-1.275720?refresh_ce (discussing Italian Supreme Court case that also ruled in favor of individuals’ right to be forgotten). In the Italian case, the public’s right to know was set at just two-and-a-half years, at which point a newspaper could be required to take down or anonymize the relevant information. Id. See also Dawn Carla Nunziato, The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten, 39 U. Pa. J. Int’l L. 1011, 1022–31, 1059–64 (2018) (discussing spread of right to be forgotten in various countries).

46 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) (Google Spain Case), 2014 ECLI:EU:C:2014:317 ¶ 80.

47 See Balkin, Free Speech in the Algorithmic Society, supra note 30, at 1174 (making a similar point).
In response, Google and other companies that are subject to such requests, have established their own internal review processes. At Google, each request is subject to a review that takes into account the validity of the request, the content at issue, the identity of the requester, and the source of the information. But whereas Google, via its transparency reporting, provides anonymized examples of a subset of the kinds of requests it receives, there is no public record of the decisions. Any public record that included names or details would itself violate the right to be forgotten. As a result, past decisions by companies like Google do not and cannot have formal precedential value.

As of September 2019, some four years after the right was announced and implemented, Google received delisting requests that covered over 3 million URLs and delinked 45% of these. According to Google’s internal data, the top 1,000 requesters generated some 15% of the requests—most of which were initiated by law firms and reputation management services. Between May 2014 and December 2018, Microsoft, which manages Bing, the second most-widely used search engine, received more than 29,000 requests covering more than 89,000 URLs and removed approximately 43%. If a delinking request is denied, individuals can appeal to the relevant Data Protection Authority (“DPA”) in their jurisdiction.

---

50 Id.
51 Id.; see also Richards, supra note 36 (finding that Bing is the second largest search engine globally; Google is the largest).
52 DPAs, often backed by courts, have adopted far-reaching interpretations of the right. In April 2018, for example, a businessman convicted of conspiracy to account falsely won the right to have references to his 1990s-era case and conviction delinked from Google’s site. See Jamie Grierson & Ben Quinn, Google Loses Landmark ‘Right to be Forgotten’ Case, Guardian (Apr. 13, 2018), https://www.theguardian.com/technology/2018/apr/13/google-loses-right-to-be-forgotten-case. As another example, New York Times reported that an article about a 2002 U.S. court decision to close down websites accused of selling an estimated $1 million worth of unusable Web addresses—part of a case that ultimately settled—was delisted from certain Google searches, pursuant to the right to be forgotten. See Noam Cohen & Mark Scott, Times Articles Removed from Google Results in Europe, N.Y. Times (Oct. 3, 2014), https://www.nytimes.com/2014/10/04/business/media/times-articles-removed-from-google-results-in-europe.html.
Conversely, if the request is granted, there is no follow-up review. The request is granted, there is no follow-up review. There is no countervailing “right of the listener” or “right to information.” Rather, the link is simply no longer available in response to a search of the particular data subject’s name.

The GDPR, which went into effect in 2018, codifies and entrenches the right (labeled the “right to erasure”), applying it to all entities that “offer[]” goods and services in the EU or “monitor[]” the behavior of EU residents, even if the entity is located outside the EU. The GDPR also expands the scope of application of this right to cover a range of additional online providers, in addition to the search engines, covered by the CJEU’s Google Spain decision. Failure to comply can result in fines of up to 4% of an entity's global revenue.

But while codifying and expanding the right, the GDPR—like the Google Spain case—did not specify the geographic reach of the substantive obligation that is imposed. Initially, Google responded by delisting the information if accessed from the European Google search domains (google.fr, google.de, google.es, etc.), but leaving it accessible elsewhere, including on google.com. Over time, this approach has evolved. Google

54 Google has adopted a practice of notifying the relevant webmaster that the link will be taken down, without specifying the reason why or individual who requested that. But the Spanish Data Protection Authority has fined Google for this practice, asserting that telling the webmaster about the decision itself violates the data subject’s right to privacy. See David Erdos, Communicating Responsibilities: The Spanish DPA Targets Google’s Notification Practices when Delisting Personal Information, Inforrm’s Blog (Mar. 17, 2017), https://inforrm.org/2017/03/21/communicating-responsibilities-the-spanish-dpa-targets-google-s-notification-practices-when-delisting-personal-information-david-erdos.

55 GDPR, supra note 19, art. 3(2), (defining the jurisdictional scope); id. art. 17(1)(a) (protecting the “right to erasure” defined as right to have personal data deleted that is “no longer necessary in relation to the purposes for which they were collected or otherwise processed”). For an excellent discussion of the jurisdictional reach of this provision, see Kurt Wimmer, The Long Arm of European Privacy Regulator: Does the New EU GDPR Reach U.S. Media Companies? Spring 2017 Comm. Law. 16, 16–19, https://www.cov.com/-/media/files/corporate/publications/2017/09/the_long_arm_of_the_european_privacy_regulator_does_the_new_eu_gdpr_reach_us_media_companies.pdf.


57 GDPR, supra note 19, art. 83.

58 According to Google, some 97% of French Internet users accessed the site using a European domain name. But the French DPA, backed by an entity made up of data protection officers from across the EU, deemed this kind of geographically-segmented implementation insufficient. See Carol A.F. Umhoefer & Caroline Chancé, Right to Be Forgotten: The CNIL Rejects Google Inc.’s Appeal Against Cease and Desist Order, Privacy Matters (Sept. 22, 2015), https://s3.amazonaws.com/documents.lexology.com/05011630-4179-42dc-b175-
now employs geoblocking to restrict access if, based on IP address, the search originates from anywhere in the EU—regardless of the particular domain name used. If, however, someone deemed to be outside the EU searches for the affected individual's name, the information is still accessible. Google asserts it can make these geographic determinations with about 99% accuracy.  

But this kind of geographically segmented response was deemed insufficiently protective by the French DPA. The French DPA argued that the right to be forgotten is a fundamental privacy and data protection right. In order to protect the data subject’s interests, Google should be required to remove the links from all domains, regardless of the place of access. The French DPA fined Google one hundred thousand Euros for failing to do so. And the issue was ultimately referred to the CJEU—pitting the French, Italian, and Austrian governments, all of whom back the French DPA in its quest for orders with global reach, against the Irish, Greek, and Polish governments, European Commission and a handful of non-profits, all backing Google in the argument that implementation was sufficient if applicable across the EU.

---


61 Id.

In a September 2019 judgment, the Court ruled in favor of Google, ultimately concluding that EU law does not mandate delinkings with global reach. In reaching this conclusion, the Court emphasized that protection of personal data is not an absolute right, but rather one that needs to be balanced against other rights—in this case freedom of expression the rights of the public in accessing information online. The Court further noted that even within the EU, Member states weigh the balance differently. Many countries outside the EU do not recognize an equivalent right to be forgotten at all. The Court thus concluded that, absent clear indication to the contrary, such as specification about how the EU rules would be reconciled with the divergent perspective of foreign nations, the EU rule would be presumed to have EU-wide application only. It could not be interpreted to mandate global delinkings. The Court nonetheless indicated that the EU law could be rewritten to encompass such a mandate. And it explicitly stated global mandates could still be issued, so long as they were grounded in national as opposed to EU law.

Meanwhile, the issue extends far beyond the EU. Russia, Turkey, Mexico, Colombia, and India all have provided for a right to be forgotten as well, whether through legislation or by recognition in the courts—also leaving open the question of geographic reach.

from the Internet (it can be found at the original source), nor allow it to dominate the impression of the aggrieved individual.

63 Judgment, Google v. CNIL, ¶ 64.
64 Id. ¶ 60, 67.
65 Id. ¶¶ 60, 67.
66 Id. ¶¶ 59, 67.
67 Id. ¶ 64.
68 Yargıtay Hukuk Genel Kurulu, Esas No. 2014/4-56, Karar No. 2015/1679 (June 17, 2015) (applying the right to be forgotten in Turkey); Nunziato, supra note 45, at 1059–63 (discussing spread of right to be forgotten in various countries); Susana Vera, Russia’s ‘Right to Be Forgotten’ Bill Comes into Effect, RT (Jan., 1, 2016), https://www.rt.com/politics/327681-russia-internet-delete-personal. An analogous right also has been extended to non-EU countries of Lichtenstein, Norway, and Switzerland, even though they are not covered by the GDPR or the CJEU’s right to be forgotten ruling. See Bertram et al., supra note 48, at 2. It is not far-fetched to think that some such countries might apply the right to undesirable, but truthful, information about political figures. Or as a means of covering up illegal or abusive incidents that powerful figures want to suppress. This would make it increasingly difficult to hold political leaders and abusers to account—potentially on a global scale. Catalina Botero Marino et al., Democracy in the Digital Age 11 (2017),
B. THE AUSTRIAN DEFAMATION CASE

In 2016, a Facebook user shared an article, which showed up as a thumbnail, including the title and brief summary of the article and photo of Ms. Glawischnig-Piesczek, along with commentary calling her a “lousy traitor,” “corrupt oaf,” and “member of a fascist party.” The article described the Green Party’s support for refugees. Ms. Glawischnig-Piesczek deemed this defamatory speech and demanded that Facebook take it down. Facebook refused, and Ms. Glawischnig-Piesczek took Facebook to court. The lower court demanded that Facebook take down the specific post. It further ordered that Facebook remove any other posts with an image of Ms. Glawischnig-Piesczek that contained the same allegations or “equivalent content,” thereby demanding that Facebook proactively monitor its site and both identify and determine what constituted a sufficiently similar critique to justify a takedown.

Facebook took down the specific identified post. But it objected to the obligation to monitor and take down additional posts, and the case worked its way up to the Austrian Supreme Court. The Supreme Court upheld the lower court’s determination that the user’s post was defamatory, but referred a set of critically important enforcement-related questions to the European Court of Justice—asking about both the permissible scope and geographic reach of takedown orders under EU law.

Specifically, the Court asked the CJEU to assess the following key questions: In addition to being required to take down a particular post deemed unlawful, can service providers be ordered to look for and remove “identically worded” information? Can they be required to do so with respect to “equivalent” information as well? And as in the right to be forgotten case,

https://www.thedialogue.org/wp-content/uploads/2017/11/Democracy-in-the-Digital-Age_FINAL-1.pdf (emphasizing the importance of the “right to the truth,” which depends on access to information, for victims of human rights violations). Even within the EU, Google reports that some 7% of requests to date have come from either a public figure, politician, or governmental official. Bertram et al., supra note 48, at 2, 7. See also Advocate General Opinion, Case C-507/17, Google LLC v. Commission Nationale De L’Informatique et Des Liberties, 2019 ECLI:EU:C:2019:15 ¶¶ 44, 61 (warning of the “danger” that the European Union will make information inaccessible in third countries and raising concerns about the risk of contagion and “race to the bottom, to the detriment of freedom of expression, on a European and worldwide scale”).


70 Id.

71 Id. ¶¶ 13-14.

72 Id. ¶ 14.

73 Id. ¶¶ 16–17.

74 Id. ¶¶ 14–15.

75 Id. ¶¶ 16–19.

76 Id. ¶¶ 19–22; Lomas, supra note Error! Bookmark not defined..
the CJEU was asked to assess geographic reach: Can the takedown and any monitoring obligations be imposed globally? Yet, the issue was framed very differently than in the right to be forgotten case—and therefore the two answers need not be the same. In the right to be forgotten case, the court is being asked to affirmatively define the geographic scope of an individual right provided for EU law. The Austrian Facebook case, by contrast, asks what, if any, limits EU law places on the Austrian court order, including limits that go to the geographic reach.

In an October 2019 ruling, the CJEU concluded that national courts could do exactly what Ms. Glawischnig-Piesczek sought. They could issue specific take-down orders; they could demand the monitoring for identically worded posts; and they could do the same for equivalent posts. The first piece of the ruling was not particularly surprising; there is nothing in EU law that would explicitly preclude national courts from demanding global takedowns of illegal content with geographic reach. As the Court pointed out, such limits come from international law, not EU law.

But the second part of the opinion was both surprising and troubling, indicating among other things excessive faith in and a misunderstanding of the technology at issue. Specifically, in concluding that courts could demand companies monitor for and take down “identical” and equivalent” posts, the Court analyzed away the seemingly applicable limits in EU law, thus setting the stage for EU member states to potentially issue broad-based takedown and monitoring obligations with global reach.

Here, the key law is the EU’s e-Commerce Directive, which deals with questions of intermediary liability, among other things. It immunizes service providers for liability associated with content hosted on their service absent “actual knowledge” of illegal activity or information and failure to remove or disable access to such information once they learn of the illegality. And it further specifies that while service providers can be court-ordered to terminate or prevent such an infringement of law, it is impermissible to “impose a general obligation . . . to monitor” in the course of doing so.

These requirements seem, on their face, to preclude the imposition of an obligation to look for and take down content beyond a particular post, webpage or other specifically identified piece of content that is deemed to contain illegal content. The EU court got around this, however, by emphasizing that while the e-Commerce Directive precludes general

77 Case C-18/18, Eva Glawischnig-Piesczek v. Facebook Ltd. (Advocate General Facebook Opinion), 2019 E.C.R. ¶ 22
78 Judgment, Case C-18/18, Eva Glawischnig-Piesczek v. Facebook Ltd., ¶ 53.
79 Id. (emphasizing that any worldwide injunction must come from international law).
83 Id. art. 14(3), 15(1).
monitoring, it does not preclude monitoring associated with a “specific case.” And it concluded that general monitoring obligations were permissible so long as they were derived from facts associated with particular, specific cases. Essential to this conclusion was the Court’s conclusion that providers would be able to monitor for and take-down the kind of identical and equivalent content covered without having to engage in “independent assessment.” The Court seemed to thus recognize that an order which required “independent assessment” would run afoul of the e-Commerce Directive’s prohibition on general monitoring. And it presumed that companies could implement these kinds of orders via “automated search tools and technologies.” In other words, the task of ferreting out equivalent content could be tasked to the machine, without requiring human engagement or independent judgment calls.

But the kind of monitoring envisioned by the Court is not nearly as automatic and simple as the Court assumed. At a foundational level, it is not at all clear that the definition of “equivalent” speech could be defined with adequate specificity to avoid independent judgment. What if the same language, but no photo? Or a different photo? What if two out of the three critiques are quoted—“lousy traitor” and “corrupt oaf”—with no mention of alleged fascist tendencies? The possible permutations are endless. For the court to define what is equivalent—what the CJEU defined as postings “essentially conveying the same message”—with sufficient specificity seems close to impossible. As a result, a platform like Facebook would almost inevitably be forced to engage in independent assessment to determine what is covered.

But even if the scope of equivalent content is somehow sufficiently specified, the context matters. Even the same exact words could convey a very different message if the context is different. What if the words are used not a critique of Ms. Glawischnig-Piezczek, but a parody? Or a critique of her critics? Or as part of an academic article discussing and analyzing the scope of European defamation law? As sophisticated as artificial intelligence is and is likely to become, it will never be able to effectively make this kind of fine-

84 Id. Par. 34
85 Id. Pars. 45-46.
86 Id. Pars. 45-46.
87 Id. Pars. 46.
89 Judgment Facebook Case ¶ 41.
tuned distinction required to assess the range of possible meanings. The only way to effectively do so is to put human beings in the position of monitors and analysts; in fact this is precisely why companies like Facebook and others have hired tens of thousands of human content-moderators to review flagged posts. Such kind of human monitoring requires exactly the kind of independent assessment that the Court rightly concluded could not be required and implicates both speech and privacy concerns and that the e-Commerce Directive rightly seeks to protect against.

Alternatively, platforms could do exactly what the court suggests—take down any post with a particular combination of words and images without any assessment of context or meaning. But this would almost certainly sweep in large quantities of what even the Austrian Court or any other court imposing this kind of order would concede is totally harmless and legitimate speech, albeit while avoiding the need for independent review. The risk, however, of over-inclusiveness—and thus over-censorship—is considerable.

Some will undoubtedly note that Facebook and other social media companies already engage in targeted monitoring of their sites for the purpose of selling ads, and that therefore they have no grounds to object to the kind of monitoring obligation being suggested by the Austrian Court. But there is a difference in kind between the monitoring done for targeted advertising purposes and that done for targeted takedown decisions for taking down allegedly defamatory speech. With respect to targeted advertising, there is no major social cost to being over-inclusive. There is, as a result, little harm done if algorithms lump those intrigued about a particular pair of shoes with those lamenting their unattractiveness. It just means that some people who don’t want ads for a particular pair of shoes may get them nonetheless.

There is, by contrast, a significant social harm to over-inclusiveness with respect to takedowns and delistings that cover political speech in ways that cannot distinguish between defamation and parody. The risk is an ossification of debate and dialogue, raising the kind of global censorship concerns that the Advocate General warned against in the right to be forgotten case. The only way to avoid this is for platforms need to engage deeply with the content and context in order to make the truly nuanced kind of decisions required—thereby raising the concerns about general monitoring that the e-Commerce Directive was meant to protect against. Moreover, targeted advertising itself is coming under attack.  

---

90 See, e.g., Julia Reda, When Filters Fail: These Cases Show We Can’t Trust Algorithms to Clean Up the Internet, Julia Reda (Sept. 28, 2017), https://juliareda.eu/2017/09/when-filters-fail/.

to search for and take down user content runs counter to the prevailing zeitgeist, adding to privacy intrusions that are already raising concerns.

Importantly, the CJEU opinion does not mandate or promote such orders. It simply opens up the possibility that member courts can issue them without running afoul of international law. National courts will—and must—take into account all of these considerations, so as to avoid the kinds of general mandates prohibited and excessive censorship that could result. Part IV provides some guidance as to key factors that courts should take into account, ultimately concluding that while global takedown mandates as to specific, identified content may be permissible in specific cases, global monitoring and keep off obligations almost never are.

C. THE NEW SOUTH WALES TWITTER CASE

An interesting yet little-commented case out of the Australian courts showcases yet another instance of a court imposing a global take-down obligation on a third-party. Specifically, the Supreme Court of New South Wales ordered Twitter to take down allegedly defamatory content. It further ordered Twitter to prevent those responsible from opening other accounts and posting any other content, whether defamatory or not. Both obligations were imposed on a global scale.92

The case stems from the anonymous plaintiff’s claim (labeled X in the opinion) that an unidentified person stole his confidential financial information and disseminated it on Twitter, impersonating his business partners in the process.93 Once alerted to these facts, Twitter removed the initially offending accounts.94 Subsequently, however, plaintiff informed Twitter that his confidential financial information had been disseminated via other Twitter accounts. This time, Twitter did not take action on either the tweets or accounts from which the tweets were disseminated.95 The accounts did not violate Twitter’s anti-impersonation policy.96

The plaintiffs sued, demanding that Twitter both remove and prevent the publication of the identified, offending material—and do so anywhere around the world, regardless of where the tweets were posted or accessed.97 The plaintiff further demanded that Twitter remove any accounts that were used to disseminate such material. And he demanded that Twitter prevent the account owners from opening up alternative accounts or posting further tweets, irrespective of the content of the tweets.98


93 Id. ¶¶ 5-6, 8.
94 Id. ¶¶ 6, 8.
95 Id. ¶¶ 10, 12.
96 Id. ¶ 10.
97 Id. ¶ 29.
98 Id.
Twitter objected to the court’s jurisdiction, did not appear in court, and instead sent an email from its support team (support@twitter.com) raising objections—including a concern about the feasibility of doing the kind of proactive monitoring that was required. 99

The Supreme Court of New South Wales rejected Twitter’s concerns and ruled in favor of the plaintiffs. 100 Specifically, the court concluded that global removals were necessary to protect the right at stake. 101 The court also concluded that that the pro-active monitoring and takedowns were well within Twitter’s competence, as exemplified by separate monitoring allegedly done for content “relat[ed] to issues of national security and classified intelligence” and spam. 102 The court further determined that once the users demonstrated their “malevolent credentials” it was fair game to keep them off Twitter, presumptively forever. 103 In the court’s words: “It could not be assumed safely that the content of any future tweets from the same source will be innocuous.” 104

This is yet a new kind of ‘keep-off’ order based on the person speaking as opposed to the content being communicated. If effectuated, it would operate as a total ban on Twitter use by those who had previously engaged in the alleged misconduct. The ban applies even to tweets that had nothing to do with the plaintiff or the plaintiff’s financial situation. As the Court itself put it—in an attempt to explain why this did not amount to content-based censorship—the “gist of the orders in relation to future tweets and future accounts, relates not to content but to user identity.” 105

As with the Austrian case, this order poses an ongoing monitoring obligation on Twitter—requiring it to play an active, editorial role in monitoring and restricting future tweets by the alleged offenders. It thus goes even further than the Austrian case in a key way—demanding the takedown of particular content and the blocking of specific users.

D. Equustek v. Google

The Equustek case presents another instance in which governments and companies are fighting about the reach of content takedown orders. The dispute is between Google and Equustek, yet arose out of a case that did not involve Google at all. 106 The underlying action arises out of an intellectual property case involving companies that manufacture networking devices that enable complex industrial equipment made by one manufacturer to

99 Id. ¶¶ 3, 35.
100 Id. ¶ 55.
101 Id. ¶¶ 29, 34.
102 Id. ¶¶ 36, 43.
103 Id. ¶ 37.
104 Id.
105 Id. ¶ 41.
communicate with equipment made by a different manufacturer.\textsuperscript{107} Canadian-based Equustek accused Datalink, which at the time operated in Vancouver, of manufacturing and selling a competing product using Equustek’s trade secrets and manufacturing and selling a competing device online.\textsuperscript{108} Equustek further alleged that Datalink advertised the sale of Equustek’s products, but then in fact delivered its own competing product in what Equustek labeled a “‘bait and switch.’”\textsuperscript{109} In response to Equustek’s allegations, the trial court ordered Datalink to return Equustek’s source code, stop referring to Equustek on its websites, and to direct interested customers to Equustek rather than selling them its own competing device.\textsuperscript{110} Datalink failed to comply and the court issued a further order that prohibited Datalink from selling its products online.\textsuperscript{111} In response, Datalink fled the jurisdiction and continued to carry on its business from outside Canada.\textsuperscript{112}

Equustek sought Google’s help. After being threatened with a lawsuit, Google agreed to delist 345 webpages associated with Datalink, but did not delist the entire websites.\textsuperscript{113} Moreover, Google only delinked the sites that were accessed via google.ca. The webpages delinked from google.ca searches were still available if the searches were conducted from google.com, google.fr, or any other access point.\textsuperscript{114}

Equustek filed a court case against Google, arguing that Google’s actions were insufficient to protect its interests. Three key reasons supported Equustek’s claim. First, most of Datalink’s sales were to purchasers outside Canada, where the delisting on google.ca would have no effect.\textsuperscript{115} Second, even Canadian customers could (at least initially) still access the webpages by simply typing in another Google URL (such as google.com versus the default google.ca).\textsuperscript{116} Third, the delisting of webpages as opposed to websites meant that Datalink was simply able to move the offending material to alternative pages within its websites—creating what the trial court described as “an endless game of ‘whac-a-mole.’”\textsuperscript{117} Equustek obtained an interlocutory injunction that would require Google to take down Datalink’s webpages and do so on a global basis, so that no one could access them regardless of their location.\textsuperscript{118}

\textsuperscript{107} Equustek 2014, 2014 BCSC 1063 at ¶¶ 2-3.
\textsuperscript{108} Id. at ¶¶ 4-5.
\textsuperscript{109} Google Inc., 1 S.C.R. 824 at 825; Equustek 2014, 2014 BCSC 1063 at ¶¶ 4-5. Equustek further alleged that prior to the completion of the competing product, Datalink actually sold Equustek’s products but covered over the name and logo and passed the products off as their own. Equustek 2014, 2014 BCSC 1063 at ¶ 5.
\textsuperscript{110} Equustek Sols. Inc. v. Google Inc. (Equustek 2015), 2015 BCCA 265 ¶ 17 (Can.).
\textsuperscript{111} Id.; Equustek 2014, 2014 BCSC 1063 at ¶ 7.
\textsuperscript{112} Equustek 2015, 2015 BCCA 265 at ¶¶ 17-18.
\textsuperscript{113} Google Inc., 1 S.C.R. 824 at 826.
\textsuperscript{114} Id.
\textsuperscript{115} Equustek 2015, 2015 BCCA 265 at ¶ 25.
\textsuperscript{116} Google Inc., 1 S.C.R. 824, 826.
\textsuperscript{117} Equustek Sols. Inc. v. Jack, 2014 BCSC 1063, ¶ 72 (Can.).
\textsuperscript{118} Google Inc., 1 S.C.R. 824, 826.
Both the trial and intermediary courts ruled in favor of Equustek, concluding that a globally-applicable order was appropriate and necessary to protect Equustek’s interests in safeguarding its intellectual property. By a vote of 7-2, the Canadian Supreme Court affirmed, describing Google as the “determinative player” in allowing the harm to continue.\footnote{Google Inc. v. Equustek Sols. Inc., [2017] 1 S.C.R. 824, 826, 828 (Can.).} Akin to the CJEU in the right to be forgotten case, the court emphasized Google’s prominent role in the dissemination of information online, noting Google was the search tool of choice for some 70–75% of Internet users worldwide.\footnote{Id. at 837.}

The Canadian Supreme Court also assessed scope of the injunction. It concluded, as did the two lower courts, that the injunction had to be global to be effective. In the court’s words: “The Internet has no borders—its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates—globally.”\footnote{Id. at 845.}

The court further noted that even though the effect of the injunction was global, the burden on Google was minimal. It could achieve a global delisting from its headquarters in California, with minimal effort and cost.\footnote{Id. at 846.}

Finally, the court considered and rejected Google’s comity-based claims regarding the risk of legal conflict with foreign law. First, the court emphasized that it was not asking Google to monitor content (in contrast to the Austrian Facebook and Australian Twitter cases), but was instead being ordered to delist specific, identified websites.\footnote{Id. at 848.} The court noted that Google regularly engages in precisely this kind of global takedowns with respect to child pornography, hate speech, and copyright violations.\footnote{Id. at 848–49.}

Second, the court emphasized that the speech at issue was not the kind of speech that interfered with “core values” of other countries, including freedom of expression concerns.\footnote{Id. at 846–47.} Rather, it involved the facilitation of the unlawful sale of goods—speech that most countries would deem a “legal wrong.”\footnote{Id. at 846–47.} The court went on to note, however, that if “Google has evidence that complying with such an injunction would require it to violate the laws of another jurisdiction, including interfering with freedom of expression, it is always free to apply to the British Columbia courts to vary the interlocutory order accordingly.”\footnote{Id. at 847.}

Two out of the nine justices dissented. The dissenters emphasized three issues: First, they warned that the injunction, while labeled interlocutory, was final in effect. Id. at 828, 852. Second, they emphasized that Google did not “aid or abet” Datalink, but merely “inadvertently facilitat[ed]” the harms committed by Datalink. Id. at 829, 860. Third, they concluded that the injunction would be insufficiently effective to be justified, particularly given Datalink’s websites could still be found and accessed via other search engines, links, email, and social media. Id. at 860. These
Defeated in the Canadian courts, Google turned to the United States. Google argued that the order violated its First Amendment rights, Section 230 of the Communications Decency Act (CDA), and principles of international comity given the global reach of the Canadian order. In a November 2017 ruling, a U.S. district court granted a preliminary injunction preventing enforcement in the United States; a month later, the court made the injunction permanent.

The U.S. district court relied on Section 230 of the CDA in support of its ruling. Specifically, the court ruled that Google was covered by the immunity provisions in CDA 230, which protect online information service providers like Google from civil liability for the information on their sites. As result, the court determined that Equustek could not have obtained the kind of injunction it received in the Canadian courts had Equustek filed in U.S. court instead. The court further concluded that the Canadian order “undermines the policy goals of Section 230 and threatens free speech on the global internet.”

But both the court’s reasoning and its result are questionable. Section 230 of the CDA provides immunity for providers for their decisions to take down—or keep up—content. It does not say anything about whether and to what extent a court or government can order such a delisting or delinking decision; such limitations come from the First Amendment, not CDA 230. Yet, the court did not directly reach Google’s First Amendment

dissenters also noted that the “worldwide effect” of the injunction “could raise concerns regarding comity,” although did not identify any specific conflict of law and did not elaborate on what would constitute the kind of concern that justified a modification of the order. Id. at 858–61.


129 Google’s Notice of Motion and Motion for Preliminary Injunctive Relief at 6–20, Google LLC v. Equustek Sols. Inc., No. 5:17-CV-04207-EJD (N.D. Cal. Jul. 27, 2017). Google also emphasized that the order was ineffective; allegedly infringing websites were available via other search engines and social media accounts. Id. at 8–9.


131 This was a default judgment; Equustek failed to appear or otherwise defend its interests before the U.S. court. Id. at *1 (N.D. Cal. Dec. 14, 2017).

132 See 47 U.S.C. § 230(c) (1) (2012) (“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”).

133 Id. § 230(c) (2).


135 Id. at *4.
claim. Nor did it elucidate how the delinking of sites selling the products of intellectual property violations undermines free speech.

With the U.S. injunction in hand, Google returned to the Canadian courts, seeking an order lifting or, in the alternative, modifying the original injunction and limiting it to sites accessed via searches from google.ca. But the Canadian trial court refused. The Canadian court acknowledged that rescission or modification might be required if in fact there were a conflict of laws. But it concluded that, despite the U.S. court order, no such conflict existed. As the Canadian trial court put it: “[T]here is no suggestion that any U.S. law prohibits Google from de-indexing …. A party being restricted in its ability to exercise certain rights is not the same thing as that party being required to violate the law.”

And that of course is correct. Even if the U.S. district court were correct that Google could not be ordered to delist the offending websites, Google was free to do so voluntarily. If it had done so, it would not have violated U.S. law. To the contrary, it would be protected from liability by precisely the same law that the U.S. district court relied on: Section 230 of the CDA.

The Canadian trial court further noted the fact that the U.S. court declined to reach the First Amendment issue. As a result, there also was no basis to think that the injunction infringed on the United States’ “core values”—implicitly indicating that a clash of core values also might have led to a different result.

Finally, the Canadian trial court also rejected Google’s separate improvement-in-technology arguments. Since the injunction first went into effect, Google has improved its ability to geographically segment the market. Rather than simply relying on default domain names (for example, the distinction between google.ca and google.com), it now employs geoblocking based on IP address. With this new and improved technology, Canadian users could not evade the restrictions on access by simply typing in google.com; unless the user took additional steps to hide his or her location, Google would know, with a high degree of accuracy, that the search originated in Canada. And it would block access as a result. But the Canadian

---

136 Id. at *3 n.2
137 Id. at *4 (stating that requiring intermediaries to remove links to third-party materials “threatens free speech on the global internet,” without further elaboration.).
138 Equustek Sols. Inc. v. Jack, 2018 BCSC 610, ¶ 20 (Can.). In this regard, I agree with the Canadian trial court. Moreover, it is not even clear that the U.S. district got the law right. The fact that Section 230 of the CDA would preclude a U.S. court from issuing the kind of injunction imposed by the Canadian court does not preclude the United States from enforcing a foreign judgment of the type sought in this case. See also Paul Schiff Berman, _Global Legal Pluralism_, 80 S. Cal. L. Rev. 1155, 1159–60 (2007) (making this point as well).
141 Id. ¶¶ 28-29.
court concluded that improved geoblocking was a partial solution at best, given that most of Datalink’s sales originated outside of Canada.142

***

As the time of issuance, the Equustek case was the first time the highest court of any country has imposed or affirmed a takedown order with global reach. The New South Wales ruling was never brought before the Australian High Court, and in any event Twitter never formally opposed the ruling so there was never a full airing of the equities at stake.143 The French right to be forgotten case and Austrian defamation cases had not yet been decided. As a result, much commentary—at least much U.S.-based commentary—viewed the Equustek case as a bellwether for a range of other cases. The Canadian Supreme Court ruling was, among other things, called “dangerous,”144 “ominous,”145 and something to be “feared.”146 Such commentary, however, appears more focused on the precedent set rather than the specific facts of the case. There is, after all, a legitimate concern that authoritarian and repressive regimes will employ global injunctions to impose, or at least seek to impose, their restrictive views on the kinds of speech that should be available. One can easily imagine, as some commentators have, a range of different countries around the world using the power of global injunctions to stifle dissent, squelch critiques of the ruling party, and hide abuse.

142 Id. ¶ 30. The Canadian court also noted that even if the United States would not aid with enforcement, Canada could continue to take independent steps to enforce. Id. ¶ 22.
145 Daphne Keller, Ominous: Canadian Court Orders Google to Remove Search Results Globally, Stan.Ctr. for Internet & Soc’y: Blog (June 28, 2017), http://cyberlaw.stanford.edu/blog/2017/06/ominous-canadian-court-orders-google-remove-search-results-globally (describing the opinion as “ominous” and raising concerns about “the message that it sends to other courts and governments”)
146 Michael Geist, Global Internet Takedown Orders Come to Canada: Supreme Court Upholds International Removal of Google Search Results (June 28, 2017), http://www.michaelgeist.ca/2017/06/global-internet-takedown-orders-come-canada-supreme-court-upholds-international-removal-google-search-results (warning of a possible parade of horribles, including “a Chinese court order[ ] . . . to remove Taiwanese sites from the index” and an “Iranian court order[ ] . . . to remove gay and lesbian sites from the index”); see also Aaron Mackey et al., Top Canadian Court Permits Worldwide Internet Censorship, Elect. Frontier Found. (June 28, 2017), https://www.eff.org/deeplinks/2017/06/top-canadian-court-permits-worldwide-internet-censorship (discussing the troubling implications of global takedown orders for free speech). But see Andrew Keane Woods, No, The Canadian Supreme Court Did Not Ruin the Internet, Lawfare (July 6, 2017), https://www.lawfareblog.com/no-canadian-supreme-court-did-not-ruin-internet (noting that “Canada’s order has a limiting principle, that is, it “is not a limitless assertion of extraterritorial jurisdiction”).
But, assuming that accuracy of the underlying facts—that Datalink is selling counterfeit goods and/or goods derived from the theft of Equustek’s intellectual property—the countervailing public interest in being able to access the webpages selling or promoting those goods is not particularly strong. More broadly, there is a range of speech that just about everyone agrees is harmful and should be kept out of the public sphere—for example, child pornography, or bullying, appropriately defined. Takedowns based on copyright infringements run into the millions per year—implemented across all of Google, Facebook, and other providers on a global scale. And while there are legitimate concerns about inaccurate or bad faith removal demands, there also is relatively widespread agreement that certain takedowns, properly identified and scoped, are appropriate—and the only way to adequately protect key security, privacy, and intellectual property interests at stake.

Even just the four cases highlighted here identified vary significantly in terms of the substance and scope of the orders. The speech at issue ranges from political (Austrian case) to personal (right to be forgotten / Twitter cases) to commercial (Equustek). These differences matter. The scope of the underlying orders also differ significantly, in ways that significantly affects their legitimacy. The delisting of particular content from the search of a particular person’s name poses far less of a censorship concern than a takedown requirement. And there is a difference in kind between orders that simply require action with respect to specific, identified information and those that impose additional monitoring and keep off or take down obligations beyond what has been specifically identified. Monitoring and keep-off obligations themselves range in terms of how much is required to be kept off the site.

Put another way, a simple claim that all global injunctions are either good or bad fails to come even close to grappling with the competing interests and complexities. I return to this issue in Part III.

E. PAST PRECEDENT

The four cases highlighted above are, of course, not the first time in which foreign governments and U.S.-based tech companies have clashed in

---

court over free speech rights. The 2000 Yahoo! case over the sale of Nazi memorabilia—permitted in the United States but prohibited in France—raised many of the same issues. Yahoo! was ordered to restrict French residents’ access to the site. Yahoo! claimed that, based on the technology available to it at the time, it could not do so in a geographically segmented way. Thus, Yahoo! claimed the ruling in effect amounted to a global takedown order, even though in practice France was asking for a geographically segmented response. Yahoo! argued that this kind of takedown order would impermissibly interfere with free speech rights.

A U.S. district court agreed with Yahoo!, emphasizing the “challeng[es]” posed by an “Internet in effect allow[ing] one to speak in more than one place at the same time.” The U.S. district court recognized that France has the “sovereign right to regulate what speech is permissible in France.” But it refused to enforce an order that chills “protected speech that occurs simultaneously within our borders.”

Ultimately, the dispute was mooted when Yahoo! voluntarily agreed to block the allegedly offending sites, and to do so on a global basis. And the U.S. district court opinion was reversed on personal jurisdiction and justiciability grounds.

What makes this case so interesting is that the reviewing French court took precisely the tack that has been rejected as insufficient by the French Data Protection Authority in the right to be forgotten case, the anonymous plaintiff in the Twitter case, Ms. Glawischnig-Piesczek in the Facebook-Austria case, and Equustek in its Canadian case. When the French

---

148 See Paul Schiff Berman, Legal Jurisdiction and the Deterritorialization of Data, 71 Vand. L. Rev. 11, 13 (2018). (noting that many of the disputes about territoriality and data are not new; rather they are simply occurring with more frequency and perhaps urgency over time); see also Patricia L. Bellia, Chasing Bits Across Borders, 2001 U. Chi. Legal F. 35, 75–76 (2001) (discussing more broadly challenges associated with extraterritorial enforcement and regulation).

149 Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181, 1184–87 (N.D. Cal. 2001), rev'd, 379 F.3d 1120 (9th Cir. 2004), on reh’g en banc, 433 F.3d 1199 (9th Cir. 2006), and rev’d and remanded, 433 F.3d 1199 (9th Cir. 2006). Despite Yahoo!’s claim to the contrary, independent technical experts revealed that Yahoo! could block access to French residents with about 90% accuracy, while keeping the auction sites available elsewhere. Yahoo! was as a result ordered to adopt a technological solution that would restrict French users’ access. See Jack Goldsmith & Tim Wu, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD at 7–8 (2006). But Yahoo! continued to paint this as a global takedown order, arguing that it would have to restrict access on a global basis to be effective—and that this would impermissibly restrict free speech. Id. at 8.

150 Yahoo!, Inc., 169 F. Supp. 2d at 1192.

151 Id.

152 Id.


154 Yahoo! v. La Ligue Contre Le Racisme et L'Antisemitisme, 433 F.3d 1199, 1201 (9th Cir. 2006).
court ordered Yahoo! to restrict access to Nazi memorabilia, it simply asked Yahoo! to restrict access for French residents only. It did not insist on a global takedown of the auction sites. When Yahoo! said it could not do so in a geographically-segmented way, France did not say that it should therefore apply the takedowns globally. Rather, it brought in expert witnesses to establish that it would, in fact, be possible for Yahoo! to geographically segment the market and thereby restrict access to French users with about 90% accuracy. And it implicitly conceded that 90% accuracy would be good enough. Fast forward and contrast to the current disputes: Providers are offering to do precisely what Yahoo! resisted and with much more accuracy than would have been possible at the time. Yet geographic filtering with close to 99% accuracy is deemed by the moving parties in all of these cases as not good enough.

II. PROVIDER-BASED DECISION-MAKING

The four recent cases—plus the older Yahoo! case—provide examples in which companies are resisting takedown orders with global reach. Yet, in myriad ways, companies have voluntarily engaged in content based curation on a global scale. Increasingly, they too struggle with the geographic reach questions: when to impose certain speech-related restrictions across their entire platform and when to adopt regional variations in order to comply with competing laws or norms?

For years, the big U.S.-based tech companies largely approached these issues with an almost messianic First Amendment perspective, as Kate Klonick and Danielle Citron ably document in their respective explorations of the development and implementation of content moderation policies and practices employed by Twitter, Facebook, and YouTube. As these authors describe it, the marketplace of ideas was something to be celebrated. The freedom to speak online would, it was widely assumed, give dissidents a voice and lead to a range of social benefits that accompany the free flow of ideas and open debate. Censorship of any kind was to be resisted. Klonick describes how the companies were populated by individuals adopting the dominant perspective of “American lawyers trained and acculturated in American free speech norms and First Amendment law.”

But even in an era of presumed First Amendment supremacy, companies engaged in global takedowns and delistings to prevent illegal

156 See Goldsmith & Wu, supra note 149, at 7–8.
157 Klonick, supra note 31, at 1621 (noting that American lawyers steeped in First Amendment law oversaw the development of company content moderation policy); see also Danielle Citron, Extremist Speech, Conformity, and Censorship Creep, 93 Notre Dame L. Rev. 1035, 1036–1037 (2018).
158 Klonick, supra note 31, at 1621.
actions like the spread of child porn or dissemination of copyright infringing material.\(^{159}\) And over time, what was once an unwavering devotion to free speech shifted. The reality of cyber bullying, terrorist recruitment online, facilitation of sex crimes, dissemination of hate speech and economic harm perpetrated by the Internet, coupled with the reality and threat of government regulation, have resulted in increasingly robust steps to control content.\(^{160}\)

As just one measure of this, Facebook’s Community Standards now include and define 20 different categories of prohibited content, including content that depicts criminal activity, albeit with a carve-out to allow for debate about the legality of criminal activity and discussion in a rhetorical or satirical way. The categories also include content that “encourages” suicide or self-harm, although discussion of suicide and self-harm is permitted; also included are support for terrorist or criminal activity, the posting of personal or confidential information without consent, hate speech, “cruel and insensitive” content; and most nudity.\(^{161}\) Individuals and groups that engage in terrorist activity, organized violence or organized hate are categorically banned from the platform.\(^{162}\) Facebook emphasizes that these Standards “apply around the world, to all types of content.”\(^{163}\) Meanwhile, its terms of service for advertisers include 30 categories of prohibited content (including the rather amorphous prohibition on “content that exploits controversial political or social issues for commercial purposes”) and 13 categories of restricted content.\(^{164}\) Google’s terms and policies include 11 different

\(^{159}\) Copyright removal requests—and compliance—are particularly high, dwarfing that of any other area. From 2011 until July 2018, Google received requests to remove more than 3.6 billion URLs. See *Content Delistings Due to Copyright*, Google, https://transparencyreport.google.com/copyright/overview. In the last six months of 2017 alone, Microsoft received copyright notices for approximately 20 million URLs and removed some 99%. Content Removal Requests Report, supra note 52 (from the URL, select “Download Report” and “CRRR H2 2017”). Facebook received close to 255,000 requests in the time period and removed 70%. Intellectual Property, Facebook, https://transparency.facebook.com/intellectual-property/jul-dec-2017.

\(^{160}\) See Citron, supra note 157, at 1036–1049 (describing increased content controls); see generally Kaye, supra note 28.


\(^{162}\) Community Standards: Dangerous Individuals and Organizations, Facebook, https://www.facebook.com/communitystandards/dangerous_individuals_organizations.


categories, some quite broad. Twitter’s rules likewise include 14 categories of prohibited content.

Many, if not most, require nuanced assessment of context and fine-tuned normative determinations, akin to those discussed with respect to the Austrian Facebook case. How should one draw the line between discussion and encouragement of self-harm? Between satire and hate speech? Terrorist and freedom fighter? Google’s policy on violence prohibits the posting of “violent or gory content that’s primarily intended to be shocking, sensational, or gratuitous.” Yet, it acknowledges that “graphic content [may be appropriate] in a news, documentary, scientific, or artistic context.” How is context and intent assessed? Twitter’s policy on hate speech distinguishes between use of “hateful” imagery and speech on the one hand, and on the other equivalent language that is used consensually in an attempt to “reclaim terms that were historically used to demean . . . .” Application requires both nuanced line-drawing and an analysis of context.

In order to do all this work, the major tech companies employ a combination of machine flagging and human review. As of 2018, Facebook employed some 15,000 to 20,000 content moderators in over twenty content review sites around the globe. These human reviewers assess a subset of the millions of pieces of content on a monthly basis, as determined by Facebook’s policy. Facebook is not alone. YouTube employs some 10,000

---

169 Id.
individuals to moderate content. At a fall 2017 Senate hearing, legal counsel for Facebook, Twitter, and Google competed to explain how they quickly act to remove “malicious actors” from their platforms, using a combination of algorithms and human review. Google, Facebook, Twitter, and Microsoft also now share “hashes,” “unique digital fingerprint[s]” that allow them to collectively identify, and prevent posting of, what is deemed to be impermissible terrorist imagery.

Much of this provider-initiated curation is implemented globally. As explained in Facebook’s introduction to its Community Standards, the company’s general terms of service apply across its platform, regardless of where a user is located or where the information posted is made available. Companies’ community standards and codes of conduct reflect their determinations that particular speech is so damaging that it justifies removal on a global scale—whether as a means of reducing the distribution of child porn, protecting against copyright violations, avoiding bullying, or minimizing terrorist recruitment online. When, for example, Twitter banned the leader and deputy leader of a British far-right organization, Britain First, for posting numerous Islamophobic posts—some of which were retweeted by President Donald Trump—it did so across its entire platform.

---


176 See Community Standards, supra note 29.

177 See Community Standards, supra, note 21. These companies’ decisions as to what content is permitted reflect a combination of cultural values and beliefs regarding free speech and privacy, as well as responses to regulators ad threat of regulators. See Klonick, supra note 31, at 1621 (noting that for U.S.-based companies this is often done by those with First Amendment sensibilities); see also Martha Finnemore & Duncan B. Hollis, Constructing Norms for Global Cybersecurity, 110 Am. J. Int'l L. 425, 442–43 (2016) (describing the influence of Silicon Valley culture on company decision-making).

At times, however, companies will seek to accommodate local laws or norms, without imposing the restrictions across the entire platform. Consider the choice facing social media companies that operate in Thailand: either accommodate Thai law that prohibits speech that insults the monarchy or subject themselves to shutdowns of their services. Companies have responded to the Thai government’s demands, as a condition of operating there, but they often do so in a geographically calibrated way. For example, there is evidence that Facebook uses geoblocking to preclude Thai-based users from accessing posts that insult the monarchy, and that this content is still available elsewhere.\textsuperscript{179}

Even within the United States, companies have employed geoblocking to address divergent state laws. Illinois, for example, prohibits private entities from collecting, capturing, purchasing or otherwise obtaining an individual’s biometric identifier (including fingerprint, retina scan, or face scan) or information (any information based on a biometric identifier) without first informing the subject and obtaining his or her written consent.\textsuperscript{181} Texas has a similar law.\textsuperscript{182} A Google-launched app that used face-recognition technology to match users’ selfies with their museum painting doppelgangers risked running afoul of the Illinois and Texas laws. Users in Illinois and Texas do not have access to the app; Google has presumptively blocked users from these states so as to comply with those laws.\textsuperscript{183}

Such voluntary use of geographic segmentation has both benefits and costs. Geographic filtering can be a useful way to address conflicting norms and rules. It allows for segmentation of the market to accommodate local preferences, without resorting to global takedowns or global delistings. In so doing, it respects diversity of norms across borders.

But this is not always a workable solution, for both practical and normative reasons, and widespread use of geographic filtering may ultimately facilitate local censorship more than would otherwise be the case. The following elaborates on both the limits and risks of geographic segmentation.

\textbf{First}, in many cases, geographic segmentation is not sufficiently protective—or deemed to not be sufficiently protective—given the interests at stake. When, for example, the Turkish government demanded that

\textsuperscript{179} Facebook is Censoring Posts in Thailand that the Government has Deemed Unsuitable, TechCrunch (Jan. 11, 2017), https://techcrunch.com/2017/01/11/facebook-censorship-thailand/.

\textsuperscript{180} Id.


\textsuperscript{182} Tex. Bus. & Com. Code § 503.001 (2017) (Capture or Use of Biometric Identifier).

\textsuperscript{183} Dianne de Guzman, Google App Finds Museum Doppelgangers for Selfie-Takers Around the World, SFGate (Jan. 14, 2018), https://www.sfgate.com/art/article/Google-art-and-culture-app-selfie-portrait-12497912.php; Dwight Silverman, How to Get Around the Google Arts & Culture App’s Block on Texas and Illinois, Hous. Chron. (Jan. 17, 2018), https://www.houstonchronicle.com/techburger/article/How-to-get-around-the-Google-Arts-Culture-app-s-12504068.php (“Although Google has not responded to our queries as to why [the museum selfie app won’t work in IL or TX], one theory is that these two states have restrictions on how facial-recognition technology can be used.”)}
YouTube ban all videos that defamed Atatürk, Google barred access from within Turkey. Turkey found this insufficient and blocked YouTube throughout the country for two years in response.  

Each of the four cases detailed in Part I similarly present situations in which governments have deemed efforts at geographic segmentation insufficient to protect the perceived interests at stake.

Some of the concerns relate to effectiveness of the geoblocking tools themselves. Domain filtering, pursuant to which access is limited based on the country-specific search functions (such as use of google.ca for Canada) can be evaded by simply typing in a different search domain. But even more sophisticated forms of geoblocking are subject to evasion. Use of virtual private networks (VPNs) enable users to bypass geographically-based filtering or blocking and access sought-after information elsewhere. In fact, after Google introduced its facial recognition app, the Houston Chronicle wrote an article informing users how to get around the geoblocking employed in Texas and Illinois that was designed to prevent access in those states. And while Google now claims it can assess users’ location with 99% accuracy, other providers may not have the technology to do so. Moreover, restricted information that is accessible elsewhere can be emailed or otherwise shared across border in ways that are not captured by the filtering in place.

Other concerns apply even if geoblocking could operate with 100 percent accuracy. Even if the restrictions are foolproof in limiting access in a particular location, a geographically segmented response means that the information remains available elsewhere. This may not, depending on the issue and perspective, adequately protect interests at stake. In Google v. Equustek, the Canadian court found that most of the sales—and thus most of the harm—were occurring outside Canada. Even if the block of Datalink’s websites were 100% effective in Canada, this kind of geographically-segmented response would not have effectively addressed the alleged harm posed by sales elsewhere. The delisting needed to be global to be effective. And in a range of other situations—whether as a means of dealing with child porn, copyright infringement, or terrorist recruitment online—geographic-based restrictions do not adequately serve the interests at stake.

Second, there also is a perverse risk that widespread use of geoblocking will encourage and enable companies to block more content, rather than less, in ways that can facilitate domestic censorship. Companies operating across borders are more likely to resist censorship and other

---


excessive limits on speech if they are being required to restrict access on a
global basis. In such situations, local norms are subject to countervailing free
speech norms and considerations that companies need to respect elsewhere.
If, conversely, companies can respond to demands to take down or delink
content in a geographically segmented way, they need not worry about
competing norms and values. As a result, they may be more willing to comply
with government demands, particularly if refusal means loss of the local
market.

These problems are exacerbated by the fact that much of this
geographic-based filtering is done invisibly. One can go to the platforms’
terms of service and find community standards, rules on advertising, and a
whole range of general policies regarding speech online. But these are the
generally applicable rules. While several of the platforms report country-
specific decisions made in response to country-specific laws, there is no
complete listing of the various permutations and adjustments made to satisfy
local laws.187 There is as a result little opportunity for public input and
resistance.

That said, geographic segmentation may at times be the best worst
way for both companies and courts to accommodate cross-border diversity
of speech and privacy norms. I return to this in Part IV.

III. NEW KINDS OF GEOGRAPHIC RESTRICTIONS: WHO IS
SPEAKING AND FROM WHERE?

It is now well-known that Russian companies and nationals “pos[ed]
pages and groups” in order to reach U.S. audiences and influence votes in
the 2016 presidential election.188 Russian actors explicitly advocated for and

187 Facebook for example, emphasizes that “[w]hen we restrict content based on local
law, we do so only in the country or region where it is alleged to be illegal,” and it
provides information on the numbers of and general basis for local-based restrictions.
But there is no clear set of standards as to when Facebook will comply with local law
and when and on what grounds it will resist. Content Restrictions Based on Local Law,

188 United States v. Internet Research Agency L.L.C., No. 1:18-cr-00032-DLF ¶¶ 4,
to defraud the United States by impairing, obstructing, and defeating the lawful
functions of the Federal Election Commission, the U.S. Department of Justice, and
the U.S. Department of State in administering the Foreign Agents Registration Act,
conspiracy to commit wire and bank fraud, and aggravated identity theft. Id.
against specific candidates, at times endorsing or attacking candidates by name.\(^{189}\) And they engaged in targeted issue advocacy—pushing on particular issues without mentioning candidates or parties by name. Ads on Facebook, for example, preyed on fears of immigrants, sought to exploit the Black Lives Matter movement, and relied on fears of police brutality as a means of motivating would-be voters and organizers.\(^{190}\) These were a form of political speech—geared toward particular political outcomes—but without ever mentioning a particular candidate by name.\(^{191}\) Even if these efforts did not alter the outcome of an election, they have rattled the public with concerns about foreign meddling and undermined public confidence in the result.

The influence campaigns continue. Reports indicate that Russians interfered in the Brexit vote and other elections in Europe.\(^{192}\) Russia—and perhaps others—sought to influence the 2018 midterm elections in the United States as well. Many such efforts engage in relatively hard-to-detect tactics—for example, by stirring up controversy over issues rather than endorsing or working for particular candidates or parties by name.\(^{193}\) The 2019 Director of National Intelligence’s Worldwide Threat Assessment warned of ongoing influence campaigns by Russia, China, and Iran.\(^{194}\)

In the wake of these concerns, politicians and policy-makers have sought ways to limit such influence.\(^{195}\) A particularly unsophisticated effort

---


\(^{190}\) Id.

\(^{191}\) Most of the 3,000 ads did not refer to particular candidates but instead focused on divisive social issues such as race, gay rights, gun control, and immigration, according to a post on Facebook by Alex Stamos, the company’s chief security officer. Alex Stamos, *An Update on Information Operations on Facebook*, Facebook Newsroom (Sept. 6, 2017), https://newsroom.fb.com/news/2017/09/information-operations-update.


\(^{195}\) The Senate’s Honest Ads Act, for example, now has 29 co-sponsors. See Honest Ads Act, S. 1989, 115th Cong. (2017). The companion House bill has 23 co-sponsors, including 11 Democrats and 12 Republicans. See H.R. 4077, 115th Cong. (2017). The bill requires, among other things, that online platforms keep records of and make publicly available information regarding who purchased “qualified political advertisements”—defined as ads that “communicate[] a message relating to any political matter of national importance, including . . . a national legislative issue of public importance.” S. 1989, 115th Cong. § 8 (2017). This proposed legislation would empower the citizenry to assess who is speaking and the legitimacy of their speech
to address this problem was initially proposed at an October 2017 Congressional hearing. Then-Senator Al Franken grilled Facebook’s General Counsel about political ads paid for in foreign currency—seeking a commitment that Facebook would refuse any such ads bought in rubles or yuan in the future. Facebook’s General Counsel refused to make the particular promise Franken sought, noting, among other concerns, the likely ineffectiveness of such a currency-based ban.

Facebook’s General Counsel did, however, commit to barring political advertising by foreign actors. In so doing, the General Counsel implicitly agreed with the basic premise that foreign speakers should be restricted; he just disagreed that the good and bad actors could be delineated by currency.

Since then, Facebook has adopted a voluntary initiative which effectively imposes this kind of ban. In order to purchase an ad in the United States about “social issues, elections, or politics,” advertisers first must be authorized. The authorization process requires a U.S. identification card (driver’s license, state ID card, or U.S. passport) and a U.S.-based residential mailing address. In other words, only U.S. residents can purchase such ads.

The ban is substantively wide-ranging. For U.S.-based advertisers, the list of “social issues” subject to the new requirements includes twenty different categories covering just about any interesting policy issue, including abortion, the economy, education, the environment, foreign policy, health, immigration, terrorism, and more. The list even includes “values.” Facebook is rolling out analogous ad authorization requirements without outright banning it. But it is not yet law. But see Wash. Post v. McManus, 355 F. Supp.3d 272, 306 (D. Md. 2019) (granting a preliminary injunction to prevent enforcement of a similar Maryland law on First Amendment grounds); see also, e.g., Leonid Bershidsky, Russian Trolls Would Love the ‘Honest Ads Act,’ Bloomberg (Oct. 20, 2017, 11:48 AM), https://www.bloomberg.com/view/articles/2017-10-20/russian-trolls-would-love-the-honest-ads-act (highlighting some of the deficiencies in the law).

See Facebook, Google and Twitter Executives on Russian Disinformation, supra note 174 (including, in addition to the exchange with Senator Franken, an exchange with Senator Chris Coons who also raised concerns about advertisements paid for in rubles). Maryland has since passed legislation prohibiting the purchase and sale of electioneering communication in “foreign currency.” Md. Elec. Law § 13-405.2 (2018).

See Facebook, Google and Twitter Executives on Russian Disinformation, supra note 174 (exchange with Senator Chris Coons raising concerns about advertisements paid for in rubles).

Social Issues, supra note 198.


Social Issues, supra note 198.
elsewhere—similarly requiring advertisers to verify a local residency as a precondition for advertising on social issues, elections, or politics.201

These rules posed a particular challenge in the run-up to the 2019 EU Parliamentary elections. The rules require advertisers to establish that they are resident in the state in which they are advertising. But, as outlined in a letter from the Secretary Generals of the EU’s three main institutions—the European Parliament, the Council of the EU, and the European Commission—this kind of geographically-segmented approach does not account for the legitimate interest in EU-wide communications.202 Such rules thus prevented European politicians from engaging in Europe-wide campaigning, which was, for many candidates, a key way of reaching voters who were physically located within the EU but not residing in their home state. As of April 2019, it continues to ban EU-based institutions from using paid advertisements to communicate across the EU about its work.203 Facebook insisted that they had “weighed the different risks” and concluded this was the “right solution [. . . to the problem of] foreign interference.”204

Twitter has since adopted a copycat requirement in the United States, requiring certification before issuing ads that “advocate for legislative issues of national importance.”205 As with Facebook, a U.S. identification and mailing address is required.206

Legislation pending in the Senate similarly seeks to expand the ban on foreign speech, albeit in more narrow term than the Facebook and Twitter advertising policies. Whereas foreigners are currently barred from engaging in “electioneering communications”—defined as the promotion or attacking of a candidate by name207—proposed legislation would expand that ban to prohibit foreigners from addressing “an issue that is reasonably understood to distinguish one candidate . . . from another.”208 This is a potentially broad category of issues. Imagine, for example, an election in

203 Id.
204 Laura Kayali & Maïa de La Baume, EU on Facebook Ad Rules, Politico (April 16, 2019, 6:21 PM), https://www.politico.eu/article/eu-institutions-blast-facebook-over-political-advertising-rules-social-media-european-election-system/ (citing a Facebook spokesperson).
which one candidate supports climate change legislation and another opposes it; this would effectively ban foreigners from engaging in any sort of paid communication in the United States about climate-related issues—or any other issue on which there were opposing views.

If enacted, this would mark a notable—and potentially unconstitutional—expansion of current restrictions on foreigners’ speech. U.S. law also has long prohibited foreign nationals from contributing to federal, state, or local elections. U.S. law also requires persons acting as agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure of their activities, receipts, and disbursements in support of any activities of their foreign principal. And, as already stated, current law prohibits foreigners from making any expenditure that involves the express advocacy for or on behalf of a candidate or political party.

But the U.S. restrictions on foreign engagement have never extended to issue advocacy or discussion of high-profile policy issues. In upholding a ban on electioneering by foreigners, the D.C. Circuit, in an opinion authored by then-Judge Brett Kavanagh, explicitly emphasized that foreigners can engage in “issue advocacy—that is, speech that does not expressly advocate the election or defeat of a specific candidate.” Thus, it was permissible to restrict foreign nationals from engaging in “electioneering,” meaning explicit advocacy for particular candidates or political parties. But foreign nationals present in the United States could speak on the issues, so long as they are not endorsing a particular candidate or political party.

These restrictions reflect a new kind of geographic segmentation based on the geography and nationality of the speaker. They are thus distinct from geographic filtering tools discussed in Part I and II, which primarily focus on the location of the listener. This shift from speaker to listener restrictions raises additional considerations and concerns.

First, these kinds of restrictions raise a range of technological, practical, and privacy-related concerns. Geographic limitations based on listener can be implemented via geoblocking—restricting all users in a particular jurisdiction from accessing information without requiring an inquiry into their identity. It is much more complicated to discern speaker location and nationality. As the current efforts elucidate, pursuant to which would-be advertisers are required to produce specific identifying material, companies will need to gather a range of information about and documentation from would-be speakers in order to make these

213 Id.
determinations. This in turn raises questions about how such information is stored, accessed, retained, and disseminated.

Second, the world is highly interconnected. The debate within the EU highlights the problems with country-based residency requirements for a system that adopts pan-European governance. But even outside the EU context, there is a legitimate interest in being able to engage in key policy issues across borders. Policy decisions on a range of critically important matters in one country—from the environment, to troop deployments, to trade policy, to immigration policy—can have profound extraterritorial effects. Think about an environmental group just over the border in Canada that wants to weigh in on mining policies being considered in the United States that could pollute its waterways, or foreign entities seeking to showcase the benefits of U.S. continued support for NATO. As a normative matter, foreigners can and should be permitted to engage on issues that can literally determine whether they live or die, and domestic audiences should at least be made aware of those considerations, even if the foreigners cannot vote. The domestic discourse benefits from the input of foreigners who often can bring an important and valuable perspective to bear.

Third, reciprocity matters. What might be seen as a short-term benefit in protecting one’s own citizens and residents from external interference in the short-term might end up harming them in the long-term, if and when they are prevented from speaking out about policies and practices employed in other nations with negative effects in their own.

To be sure, at least as being currently implemented by Facebook and Twitter, the bans apply only to paid advertising. Foreigners can still speak; they just cannot buy paid ads on particular issues. And there are, to be sure, good reasons to be concerned about foreign efforts to engage in disinformation campaigns and otherwise influence elections—including through the effective use of targeted advertising.

But there are alternative ways to address these concerns. The kind of transparency being sought via efforts like the Honest Ads Act—which requires transparency about the source and distribution of political ads—is a good place to start. So are independent efforts like that of Steve Brill’s NewsGuard which assesses and rates news websites for credibility and transparency. And for the same reasons that paid advertising is used by adversaries, it also may be a key way to reach a desired audience for legitimate reasons as well. It is, as the EU discussion highlights, one key way in which European institutions have sought to communicate with their pan-European constituents. Advertisements allow the speaker to reach a different and much broader audience than other forms of communication; these restrictions cut off key avenues for doing so.

IV. A WAY FORWARD

214 See supra notes 200–202 and accompanying text.
215 See supra notes 196–204 and accompanying text.
Speech regulations online result from a combination of governmental and private decision-making, some of which is the topic of the kinds of high-profile cases discussed in Part I, but much more of which takes place behind the scenes via the complex and daily decisions of massive private corporations. Doing so—at least doing so well—requires an understanding of local context and culture. It requires an accommodation of conflicting norms across borders. It requires an understanding of the possible technological means and limits of those means in identifying and segregating unwanted speech. And it requires a normative vision of what is and should be permitted speech online.

In what follows, I examine the ways in which the geographic reach and content questions are inextricably linked. I then turn to issues regarding the substantive scope of the obligation being imposed; the risks of new forms of geographic limitations based on the location of the speaker as opposed to that of the listener; and questions of accountability and transparency, particularly with respect to private decision-making.

A. GEOGRAPHIC REACH

The following assesses three possible responses to the geographic reach questions presented the courts and companies on a daily basis: first, global takedowns as the default; second, geographic segmentation as the rule; and third, a middle ground, pursuant to which there is a default presumption in favor of geographic segmentation, but one that can be overcome. This of course is not an exhaustive list of possible approaches, but collectively, these options allow for an articulation of the key interests at stake.

I ultimately come down on what I call the middle view. It is one that favors a presumption of geographic segmentation—albeit a presumption that can, depending on the context and content, be overcome. It thus recognizes that not all speech claims are equivalent. In some instances, global takedowns or delistings may be the only possible means of protecting a key right or interest—something that has been implicitly recognized in the context of child pornography, extortion, and efforts to protect the dissemination of copyright-infringing material. This determination, in turn, depends heavily on content and context.

Finally, while I direct my recommendations here to the courts being asked to adjudicate between competing claims regarding geographic scope, the underlying principles can—and should—guide company decision-making as well. Moreover, for the purpose of this section, I am assuming that the orders are limited to particular, identified posts or webpages and do not include broader requirements to search for and take down additional postings or accounts. I turn to the critically important scope questions next.

i. A Presumptive Global Mandate

Under this approach, courts would, given the articulation of an interest sufficiently strong to justify a mandated takedown or delisting, apply
that obligation globally. Applying basic rules of international comity, the presumption would be overcome if and when a global order would generate a conflict of laws, thereby putting companies in the untenable position of having to break another country’s laws in order to comply with the demand for a global takedown or delisting.

Such a presumption ensures that whatever interest justified the takedown or delisting order is maximally protected. It thus serves the interests of the parties in the jurisdiction that demanded the takedown or delisting, protecting them against the risk that what is deemed impermissible content will be accessed in other jurisdictions or, via technological evasion of geographic limits, in their own. It would, in effect, result in territorial rule-making with broad extraterritorial effect.

Such an approach would, however, lead to the result of which many have warned—the most censor-prone nation setting global rules. Imagine Russia, Turkey, Thailand, or Saudi Arabia determining the scope of available content across any social media company or search engines that serves its residents. Or Poland—which for a time made it a crime to attribute Holocaust crimes to the Polish state. This would result in an impoverished global dialogue, one that stifled dissent and disagreement.

Moreover, the theoretical limit based on conflict of laws will almost never—and perhaps never—come into play. Absent some sort of must-carry obligation, takedown and delisting obligations merely compel companies to do something that they can do voluntarily. And while the “right to receive” information is codified in documents such as UN Declaration of Human Rights, European Convention of Human Rights, and Charter of Fundamental Rights of the European Union, and referred to in U.S. case law, the scope of that right is not well-defined.

There is, as a result, almost never a conflict between a takedown or delisting order and another competing legal obligation. The Canadian trial court correctly recognized this when it noted that the provisions of § 230 of the CDA did not, despite the U.S. district court’s conclusion to the contrary,

---

217 See supra Part I.D.
219 See Keller, supra note 34, at 7–10 (making this point).
generate an actual conflict of law with the Canadian order in the case.\textsuperscript{221} As a result, companies are generally not violating others’ laws when they take down content, even if doing so pursuant to a governmental or court-ordered mandate.

Finally, there are particular risks associated with governmental and court-ordered takedown and delisting mandates that countenance against a default global takedown rule, even if we all recognize that companies impose such global standards by default. As powerful as they are, companies are not monoliths. Google’s search engine has captured almost 90% share of the global market.\textsuperscript{222} Some 2.1 billion people around the world use Facebook products each day.\textsuperscript{223} But even these companies do not fully occupy the field. Even if less powerful and less effective, there are alternative means of communication, whether in the form of alternative social media sites, such as Gab, which serves a range of alt-right users; closed sites that specialize in things like the distribution of adult pornography; or other platforms that develop to serve local markets that satisfy local norms.\textsuperscript{224} So long as they do not cross the line into illegality, these alternative sources of communication can provide an alternative space for the dissemination and sharing of content that would not be allowed on some of the major tech companies’ sites. Government and court-ordered mandates, by contrast, shift the line of legality. They set standards that everyone must abide by, thus eliminating the alternative spaces for dissent and exchange of non-mainstream ideas.

Moreover, the major platforms’ community standards and company policies are themselves flexible and changeable. The companies also take action in response to consumer demands in both directions—both taking down material in response to complaints and shifting policy in response to the perception that they are engaging in excessive or biased takedowns. Government and court-ordered mandates eliminate that flexibility.

\textit{ii. A Geographic Segmentation Rule}


Under this rule, courts would mandate takedown and delisting orders in their jurisdiction only. As with any other takedown or delisting decision, providers could *choose* to apply the restrictions globally but would not be *required* to do so. This has the obvious advantage of avoiding the kind of global censorship that would result from a presumptive global mandate rule.

But there are costs to this approach as well. *First,* there is the risk that a global segmentation rule will fail in certain circumstances to adequately protect an important interest at stake—thereby falling into the trap of treating all takedown and delisting orders as one and the same. But, as articulated in Part I, the interests vary significantly based on the subject matter at issue. Orders designed to restrict dissent or discussion of uncomfortable but true historical events) implicate very different equities than private individuals’ attempts to control the dissemination of embarrassing information about themselves (the right to be forgotten). These in turn raise very different considerations than efforts to prevent the dissemination of trade secrets, copyrighted material, or stolen credit card numbers—pursuant to which there are often strong justifications for imposing orders on a global scale.

*Second,* in leaving the geographic reach decision entirely to providers, the rule effectively delegates what are critically important question about how to reconcile competing interests and norms to the private sector. There are reasons to be worried about abuse of power by governments and courts. But there are also concerns with a system in which providers are given the exclusive default power to make these decisions about how to accommodate competing norms across borders.

*Third,* somewhat ironically, global segmentation as a default rule creates its own risks of over-censorship. Companies, knowing that they only need to comply with local orders locally, may be more willing to comply with takedown and delinking orders rather than resist. At times, this may reflect a necessary, and positive, attempt to abide by and accommodate local norms. But there also is a risk that such geographic segmentation will facilitate private complicity in governmental efforts to suppress dissent, hide abuse, or cover up uncomfortable truths. If the takedown or delinking decisions do not have to be defended globally, it may become increasingly easier to comply.

iii. The Middle Ground: Presumption in Favor of Geographic Segmentation, But One That Can Be Overcome

---

225 *See* discussion, *supra,* Part I.

226 Here I refer to human rights norms rather than First Amendment norms. There are a range of speech restrictions that are prohibited by the First Amendment that are, pursuant to human rights law, deemed permissible. See, e.g., Frederick Schauer, *The Exceptional First Amendment,* in *American Exceptionalism and Human Rights* 31–38 (Michael Ignatieff ed., 2005). My concern is with content mandates that fall below the level of basic human rights norms.
Under this approach, courts will, as a default, apply takedown and delisting orders in their jurisdictions only. But this default can be overcome if there is a sufficiently strong interest at stake and such a mandate does not interfere with free speech principles, including the right to receive information, robustly identified.

This of course is not the only way to describe a possible middle ground, and it may not be the best one. However, it does represent the basic idea that, while geographic segmentation is the least bad way to accommodate competing visions of what is and is not protected speech, there are times in which global mandates are the only means of effectively protecting important interests, and the private companies’ determination of the equities at stake may not always be the best one. In other words, in some rare instances, courts can—and perhaps should—mandate global takedown or delisting orders over companies’ objections. Meanwhile, in contrast with the presumptive global mandate, this approach explicitly requires consideration of the right to receive information.

Let us now consider how this approach would play out in the four cases highlighted in Part I.

In the Austrian defamation case, Facebook would win; any takedown order could only be implemented locally. Facebook, after all, is being asked to take down what amounts to core, albeit crude, political speech. Even across Europe, there are divergent views as to the scope of permissible defamation claims. In other words, there is insufficient consensus as to the harm inflicted as well as an articulable right to express and receive what is deemed core political speech.

Similarly, there is a lack of sufficient consensus regarding the right to be forgotten to justify its implementation on a global scale, regardless of the specifics of the claim. There is not a global consensus as to either the existence or scope of the right. It has been considered and rejected in parts of South America, where there is a concern about the right being used by powerful leaders to cover up abuse. Such a right also could not be imposed in the United States without running into significant First Amendment issues. The Advocate General was therefore correct when he concluded that a global mandate fails to adequately take into account the broader “right to receive information.”

Conversely, the Canadian _Equustek_ case would be one in which the presumption would be overcome and a global mandate would be legitimate, assuming the underlying alleged facts are true, and that Datalink is selling goods derived from a theft of intellectual property. There is no

---


228 Marino et al., _ supra_, note Error! Bookmark not defined., at 6, 10, 11.

229 Advocate General Facebook Opinion, 2019 E.C.R. ¶ 60.

countervailing right to access fraudulently obtained information or counterfeit goods. Of course, even with respect to intellectual property, there is not universal agreement as to the substance and scope of particular harms. But there is nonetheless a sufficiently widespread agreement that those subjected to theft of trade secrets should be protected, plus a sufficient risk that a geographically limited delisting or takedown order will provide inadequate protection to the affected right-holder, that a global order seems at least potentially justified.

The Twitter case is slightly harder to evaluate, as there is a dearth of information as to the specifics of what is being disseminated. But if, in fact, it is confidential financial information, fraudulently obtained, then there may be a basis for global implementation. Factors to consider would be the nature of the information, the effect on the plaintiff, and the possible interests of listeners in accessing that information, which will depend in part on the identity of the plaintiff and nature of the information.

**

This approach will undoubtedly be critiqued, rightly so, for requiring courts to engage in the difficult and hard-to-ascertain analysis of what constitutes a sufficiently legitimate interest, when there is a general consensus about that interest, and whether and to what extent the right to access information is unduly harmed in a particular case. There is an undeniable amount of indeterminacy in such decision-making. For those who prefer rules over standards, this will not be a preferred approach.

But it is also worth noting that courts around the world routinely engage in analogous, fact-dependent assessments in both speech-related and other cases. Courts are routinely called upon to consider the interests and equities presented by foreign law, whether identifying the contours of customary international law, adjudicating claimed legal conflicts, assessing whether and to what extent laws with extraterritorial reach unduly invade the sovereignty of co-equal nations, or engaging in comity analysis more broadly. Moreover, the small handful of cases that ultimately make it to the courts—rather than be worked out quietly behind the scenes—are sufficiently high-profile, generally involving the kinds of high-resourced companies that can afford this kind of legal fight, such that one can assume

---

a full airing of the respective interests and considerations. While far from perfect, this intermediate approach thus has the advantage of accounting for the inevitable complexity and range of interests in a way neither a presumptive global mandate nor a mandatory geographic segmentation rule can.

B. SCOPE OF THE ORDER

The discussion so far has assumed that we are talking about takedowns and delisting requirements associated with particular, identified content. But as the discussion in Part I highlighted, many of the orders include additional requirements to search for, take down, and keep off additional content, accounts, and users beyond the particular post, article, or webpage initially identified.

These should be resisted, particularly if being imposed on a global scale. Such mandates go far and beyond takedown or delisting orders associated with particular content. They force providers into the role of unwilling editor, forced to adjudicate what is and is not sufficiently similar to justify takedowns or delistings. They violate countervailing provisions, such as that codified in the EU’s e-Commerce Directive that prohibits courts and governments from imposing a general monitoring obligation on companies.\(^\text{233}\) They incentivize over-censorship. And, they threaten privacy by requiring private actors to analyze context and content in order to assess whether particular material runs afoul of the order.

Moreover, despite the claims of some courts, this kind of filtering and ongoing monitoring is something that can be done passively and automatically, with the use of technological tools. Whereas companies can and do use digital hashes to identify and keep off particular imagery, there is no adequate tool available that enables them to accurately identify the range of content that crosses the fine line between permissible and impermissible speech.\(^\text{234}\) Unless such a mandate is very narrowly tailored to identify a particular image or article, machines alone cannot tell whether language used to vilify in one context is being used as satire or condemnation of vilification in another. That is, in fact, precisely why the major tech companies have invested so heavily in human content-moderators; they recognize that these are not decisions that can be relegated to machines.\(^\text{235}\)

Of particular concern, providers seeking to protect against ongoing liability will be incentivized to be over-inclusive in determining what constitutes impermissible analogous content, exacerbating the risk of excessive court-mandated and company-implemented censorship.

---

\(^\text{233}\) See Keller, supra note __, at 28–35 (analyzing filtering obligation in light of the e-Commerce directive).

\(^\text{234}\) Id. at 8–12; Reda, supra note __. But cf. Stuart Macdonald, How Tech Companies Are Successfully Disrupting Terrorist Social Media Activity, Conversation (June 26, 2018, 6:53 AM) (discussing Twitter’s effective use of digital hashes to interrupt terrorist activity on the platform).

\(^\text{235}\) See supra Section 1.B (discussing these issues).
Meanwhile, courts also should be wary of requirements, like that imposed in the Twitter case, which entail speaker-based bans in addition to content-based restrictions. In ordering that Twitter block the users from ever opening another account, the court effectively concluded that blocking that user from the site permanently, regardless of the content. That is an overbroad and generally unjustifiable restriction. Of course, companies do at times ban users for repeat violations of their terms of service. But that is an extreme action—justified only after there has been a repeated, ongoing pattern of abuse, notice, and failure to desist. It is not something courts should do absent extraordinary circumstances and a meaningful opportunity for the affected user to mount a defense.

C. New Forms of Geographic Segmentation

New forms of geographic restrictions based on the location of the speaker rather than the listener also raise significant concerns. Such efforts stem from legitimate concerns about foreign election interference—an issue I intend to examine in more depth in future work. For now, I simply note that quick fixes designed to limit foreign speech raise more concerns than any promised benefits. Put simply, while there are long-standing limitations on foreign coordination with particular political parties or candidates running for office there are a range of reasons why foreigners should not be precluded from speaking on policy issues. Foreigners may have significant equities at stake. Foreigners can offer valuable perspectives, adding to the robustness of the debate. Moreover, regional governance efforts, whether formalized in the EU or informal modes of cooperation across borders, benefit from, and arguably require, policy engagement and information-sharing across national borders. Furthermore, even the effort to determine who is speaking and where the speaker is located raises potential privacy concerns not implicated by other forms of geographic segmentation that can be implemented without any inquiry into the profile of the speaker or listener.

D. New Forms of Accountability

The first part of this paper focused on the small number of court cases raising questions about geographic reach. But as described in Part II, many, if not most, of the key decisions are being made by private companies that rule themselves. Court involvement is the rare exception, not the rule. Of course, private actors do not operate in isolation. They are influenced by, and also influence, the multiple powerful governments of the countries in which they operate. But whereas governments—at least the democratic ones, and at least in theory—are held accountable by voters, the public has no means of voting particular corporations in or out. Moreover, increasing concentration of the market by a handful of dominant players means that

\[236\text{ See supra section II.}\]
\[237\text{ See supra section III.}\]
users cannot readily vote with their feet; doing so may cut them off from a key information source or dominant mode of communication with friends and family. Meanwhile, users in country $A$ have virtually no say as to how a company responds to speech regulations imposed by country $B$.

This requires us to think through new and additional forms of accountability, transparency, and control. Here, too, I consider a range of different approaches, including more explicit governmental oversight, increased transparency, and privatized efforts at oversight and control.

i. External oversight

The *Google Spain* case, which announced the right to be forgotten, is remarkable for a number of different reasons. But perhaps the most notable aspect of the case is the way it entrenched and established the primary role of private search engines in adjudicating the right. Albeit consistent with EU practice in other areas, the CJEU placed on Google the specific obligation to review and adjudicate claims made pursuant to the right to be forgotten. The court could have demanded the creation of public, quasi-judicial administrative review boards, employing public officials to do the initial reviews and thereby creating a record of the decisions. The review boards would then make the decision and direct Google to delink—or not. But, instead, the court and implementing countries delegated this task to the private sector, albeit subject to administrative and court review.

In fact, one can imagine a system in which all demands to take down or delist particular information are reviewed by some sort of independent, judicial or quasi-judicial body. Such a system has the obvious advantage of increased accountability and transparency with respect to content-moderation decisions.

But, among other challenges, it would be incredibly difficult to administer. The sheer volume of takedown and delisting demands and decisions make it near-impossible to outsource to a public entity. It would be virtually impossible to impose an ex ante requirement for a takedown or delinking; the time delays would make many of the issues moot by the time any independent body were in a position to review. Alternatively, it could be administered as an appeal board akin to the system with the right to be forgotten, pursuant to which individuals first go to Google, but then can appeal any adverse decision to their Data Protection Authority. A more equitable system would need to also an opportunity for those seeking to keep content accessible to raise claims.

This too raises volume and timeliness challenges. Moreover, it only works when there is a clearly articulated set of standards for the reviewing board to administer. The right to be forgotten provides such standards in the EU, as it is now codified in EU law. But even the balancing of the data protection and privacy interests with respect to that right differs cross EU

---

238 See *infra* Section I.A (discussing this case).
239 See *Post*, *infra* note 40, at 1068–71 (making a similar point).
240 GDPR, *infra* note 13, at art. 65.
member state borders. What about hate speech, bullying, or terrorist recruitment online? A country such as Germany could adjudicate hate speech claims against their NetzDG—a law that prohibits the use of hate speech online.241 But in many other countries, including the United States, companies are permitted to, and in fact do, restrict a range of speech that is permitted under the First Amendment. By what standards would a public review board evaluate such decisions? The companies’ own standards? The First Amendment standard?

One option would be to impose a due process-type requirement on the companies—mandating that they articulate and adhere to the standards applied—and then give appeals boards the opportunity to assess whether or not the standards were applied, akin to an arbitrary and capricious review standard in administrative law. This approach would, however, still leave the substantive standard-setting to the companies. Many other practical and normative challenges would arise as well, including questions of who sits on these boards, how to manage the volume, how to take into account competing interests, and whether and to what extent decisions are implemented locally versus globally, among numerous other considerations. Here, I simply seek to identify the option—a prospect that also has been identified by others.242 Much more work is needed to elaborate and evaluate the proposed design.

ii. Privatized oversight

Absent public oversight, private actors can implement their own internally-created oversight mechanisms, and have in fact done so. The most notable development is that being pursued by Facebook. In April 2018, Mark Zuckerberg unveiled plans to create Facebook’s own internal “Supreme Court”—a sort of independent appeals board that can “make the final judgment call on what should be acceptable speech in a community that reflects the social norms and values of people all around the world.”243 The particular turn of phrase—“Supreme Court”—was unfortunate, highlighting

---


242 See ACLU Foundation of Northern California et al., The Santa Clara Principles on Transparency and Accountability in Content Moderation (2018), https://santaclaraprinciples.org/ (stating that, “[i]n the long term, independent external review processes may also be an important component for users to be able to seek redress” with respect to content-moderation decisions).

the hubris of Facebook and reflecting the enormous power that Facebook yields. But the concept is an interesting one—particularly in the absence of separate public oversight mechanisms.

In January 2019, Facebook unveiled initial plans for an independent “oversight board” for content decisions.244 There are, as Facebook itself recognized, numerous issues to work out.245 How many board members are there, and how are they chosen?246 How can one ensure their independence?247 How are cases selected for review?248 Are decisions made public?249 Do they have precedential value?250 Are they implemented in a global or geographically segmented way? How does one “ensure cultural sensitivity” and the protection of diversity, particularly if decisions are, consistent with the quest to identify shared speech norms and values, implemented globally?251 After a period of initial consultations around the globe, Facebook announced in June 2019 its initial thinking on how some of these issues should be resolved.252

In the absence of governmental oversight, this kind of self-generated external oversight holds out the promise of additional accountability and transparency. In order to satisfy these goals, decisions should be public to the greatest extent possible consistent with privacy considerations of individuals—thereby feeding back into Facebook’s internal decision-making process. They should have precedential value, providing an internal case law that can then be relied and elaborated on going forward. A clear articulation of the substantive and procedural standards relied on, grounded in human rights law but filled in to provide additional guidance, will be needed.253 Numerous other considerations need to be taken into account, many of which are addressed in Facebook’s initial report on the issues.254

---

246 Id. at 1–2.
247 Id. at 2, 4.
248 Id. at 3.
249 Id. at 5.
250 Id. at 11.
251 Id. at 7.
253 Id. (highlighting need to couple human rights law with additional standards); see also Kaye, supra note x, at 119–121 (arguing for reliance on human rights law as a foundational set of norms governing content-moderation decisions).
If designed to ensure the Board’s independence, this approach enables additional perspectives and inputs to be considered, separate and apart from those working directly for Facebook on a daily basis. If successful, it can and should be mimicked by others. And perhaps eventually, it will feed into the development of a quasi-public, quasi-independent review mechanism, thus capitalizing on the successes and failures of the private efforts and allowing for the kind of increased accountability needed.

iii. Increased Transparency

Companies also can and should commit to increased and fuller transparency about the takedowns and delistings practices and policies. This would build on and expand the current biannual transparency reporting that already exists. These reports disclose things like the number of governmental requests for data, the government making the request, and the nature of and response rates with respect to content takedowns and delistings.255

Some of these reports address geographic reach questions, but in a limited way. Facebook, for example, now details when they take down content for violating local law—that is, takedowns that are executed in a geographically segmented way.256 Twitter and Google similarly include a discussion of country-specific takedowns and withholding of content.257 They also include sample descriptions of adjudication decisions. But more details and examples would be illuminating. What is a valid ground for responding to a local takedown or delisting? Are there any limitations to compliance with local law? In what circumstances, if any, are they being asked to apply local requirements globally?

Meanwhile, as David Kaye notes, “transparency is not a one-way ratchet.”258 Governments can and should do more to be transparent about what kinds of demands they are making on the companies and why. Transparency alone will not be enough, but it is the first step to accountability and broader engagement. It is something that ought to be required.

iv. Democratic Engagement

255 See, e.g., Government Requests to Remove Content, Google, https://transparencyreport.google.com/government-removals/overview; Requests for User Information, Google, https://transparencyreport.google.com/user-data/overview. Google initiated these reports in 2010. The practice was ultimately adopted by other companies, in part because of demands made by advocacy groups and other actors. The scope of what is reported has expanded over time.


258 Kaye, supra note 28 at 124.
As David Kaye also writes, such transparency should be accompanied by greater and more decentralized engagement between the governments and companies that regulate content and the parties subject to that regulation.\(^\text{259}\) Even in the absence of formal review boards of the type being considered by Facebook, companies can and should do more to engage in multi-stakeholder discussions at the local level in all the countries in which they operate. Kaye also suggests that the companies should have “desk officers” in the countries in which they operate around the world to manage these relationships.\(^\text{260}\) Not only will this help with ensuring that a fuller range of perspectives and considerations are being considered, but it will also help answer the geographic scope questions by generating a better understanding of local context, culture, and norms—as well as differences that arise across borders.

***

To be sure, none of these recommendations are fully satisfactory. There is almost certainly always going to be an accountability and transparency deficit, as there are in democracies. But just as voters, commentators, and activists have long pushed for greater accountability on the part of governments, so too should users, commentators, and activists demand the same of private corporations. Private tech companies are, in the words of Professor Kate Klonick, the “New Governors.”\(^\text{261}\) And because they operate across multiple borders, they are in fact Global Governors. They have the power to both shape global norms and determine how conflicts across borders are mediated. We need to pay attention to how these decisions are being both made and implemented, both locally and globally.

**CONCLUSION**

In a globally connected world, a speaker in State \(A\) can be heard almost instantaneously in State \(B\). The listener in State \(B\) may not know the identity of the speaker, or have any idea that the speech has crossed multiple borders on its way. In many ways, this is the promise of a free and open Internet—with ideas and the exchange of information untethered to national, territorial boundaries. But the free and open Internet is not the utopian cyberspace once envisioned. Sometimes the speech is harmful. Or deemed harmful. And in response, governments—sometimes directly, and sometimes indirectly—seek to set limits on what can be said and disseminated online. Oftentimes there is consensus as to these rules. However, norms both conflict and diverge sharply across borders, raising important questions as to who gets to set the rules. This is apparent in the key court case that directly raise the issue, but also in a host of other determinations—and battles—playing out online. Whose vision of what

\(^{259}\) Kaye, supra note 28 at 118–120.

\(^{260}\) Kaye, supra note 25, at 118.

\(^{261}\) See Klonick, *supra* note 31, at 1603.
constitutes permitted speech controls? The United States’? Europe’s? China’s? And to what extent can these countries impose their vision beyond their borders?

This Article examines these conflicts and proposes a way forward—one that seeks to respect and protect divergent norms, albeit with baseline protections in place. Yet, it also recognizes that the free flow of information across borders sometimes requires global restrictions in response. While geographic filtering and geoblocking provide a promising way to respond to and respect diversity across borders, at times such geographic segmentation fails to sufficiently protect valid interests. New forms of transparency and accountability are also needed to account for shifting power structures and protect against the risk of an increasingly restricted discourse. This analysis is thus directed at both the state regulators and the multinational tech companies that are increasingly able to set or delimit global norms in ways that single states are unable to achieve on their own.