Here, There, or Everywhere? Assessing the Geographic Scope of Content Takedown Orders

Alicia Solow-Niederman,[1]
Francisco Javier Careaga Franco,[2]
Nani Jansen Reventlow[3]*, and*
Vivek Krishnamurthy[4]

Working Paper— March 27, 2017

1. OVERVIEW: SETTING THE STAGE

In theory, the internet may be a space free from the bounds of sovereign territories,[5] and much of its promise indeed springs from its seemingly boundless capacity for interconnection and innovation, unconstrained by physical limitations. In practice, however, the issue is more complicated. There is a roiling debate on whether legitimate national laws and preferences should be applied and enforced online by extending the doctrine of territoriality to digital spaces. This conversation implicates core public international law doctrine and freedom of expression values, including the right to access information. Cross-border content takedown requests put the internet's territorial fault lines into especially stark relief.

Ongoing contestation around the reach of the so-called "right to be forgotten"[6] (RTBF), a much-debated concept that has emerged in the

---

[1] J.D. Candidate, Harvard Law School, Class of 2017.
[2] LL.M Candidate, Harvard Law School, Class of 2017
[3] Associate Tenant, Doughty Street Chambers & Fellow, Berkman Klein Center for Internet & Society, Harvard University.
[4] Assistant Director, Cyberlaw Clinic, Harvard Law School & Berkman Klein Center for Internet & Society, Harvard University.
[5] For the classic iteration of this idea, see John Perry Barlow, A Declaration of the Independence of Cyberspace (Feb. 6, 1996), https://www.eff.org/cyberspace-independence ("Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.").
[6] Unless otherwise noted, this analysis treats "right to be forgotten" as analogous to the "right to be delisted" or "right to be de-indexed."

wake of the 2014 *Costeja*[7] case, stands out as an especially prominent fault line[8] surrounding national sovereignty and jurisdiction in the digital era. On one hand, a nation–state may pursue a content takedown request in a legitimate effort to ensure that its citizens are not exposed to material that would undermine the substantive objectives that its own laws and policies advance. On the other, overbroad enforcement of content takedown requests carries at least two risks. First, it may threaten access to information and freedom of expression for citizens of that nation-state, especially when the requests are served on intermediaries that may wish to avoid liability[9] and thus may take down content without much resistance or even preemptively.[10] Additionally, if

---

[7] C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, 2014 E.C.R., http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN. *See also* CNIL, *Right to be Delisted: The CNIL Restricted Committee Imposes a €100,000 Fine on Google* (Mar. 24, 2016), https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google (interpreting the European Supreme Court's *Costeja* decision and concluding that the requested de-indexation must be applied globally to protect citizens' rights).

[8] For an examination of how this debate is unfolding in the dispute between Google and France's data protection agency, CNIL, that underscores how one nation's cross-border demands can threaten global freedom of speech, see Nani Jansen Reventlow, Vivek Krishnamurthy, & Christopher T. Bavitz, A French Court Case Against Google Could Threaten Global Speech Rights, Wash. Post (Dec. 22, 2016), https://www.washingtonpost.com/news/global-opinions/wp/2016/12/22/a-french-court-case-against-google-could-threaten-global-speech-rights.

[9] The dynamics around the United States' DMCA Safe Harbor provisions illustrate how companies may remove content to avoid potential liability. See DMCA Safe Harbor, Lumen, https://www.lumendatabase.org/topics/14#QID127 (last visited Mar. 6, 2017) ("Section 512 of the Digital Millennium Copyright Act (DMCA) protects online service providers (OSPs) from liability for information posted or transmitted by subscribers if they quickly remove or disable access to material identified in a copyright holder's complaint.").

[10] As a descriptive matter, many industry codes of practice and voluntary agreements reflect corporate choices to align business practices with government objectives in ways that may result in content filtering or removal of categories of content without more granular consideration of or adjudication of specific cases. *See, e.g.*, Ernesto Van der Sar, *Search Engines and Rightsholders Sign Landmark Anti-Piracy Deal*, TorrentFreak (Feb. 20, 2017), https://torrentfreak.com/search-engines-and-rightsholders-sign-landmark-anti-piracy-deal-170220/ (describing the official announcement of "the world's first anti-piracy agreement between search engines and rightsholders," including Google, Microsoft Bing, and creative organizations, after years of conversations with U.K. policymakers). Another example is the recently failed Copyright Alert System, a voluntary agreement between copyright owners and IPs that created a "6-strikes" regime that emulated the DMCA+ graduated response model. *See* David Kravets, *RIP, "Six Strikes" Copyright Alert System*, Ars Technica (Jan. 30, 2017, 2:50 PM), https://arstechnica.com/tech-policy/2017/01/rip-six-strikes-copyright-alert-system/. In addition, many intermediaries are using algorithms to filter and block, and YouTube's Content ID even allows qualifying content producers to earn advertising revenue from infringing content. *See How Content ID Works*, YouTube, https://support.google.com/youtube/answer/2797370?hl=en (last visited Mar. 23, 2017).

one nation's content takedown enforcement request spills across geographic borders and affects citizens of another country, it undercuts or outright contradicts critical international law presumptions of territoriality and principles of international comity. Despite the contemporary reality of such issues, it is not clear that courts are well-positioned to resolve them in a way that respects national sovereignty, both within one country and across borders, while simultaneously protecting global access to information and freedom of expression.

Indeed, the debate regarding the RTBF represents but one instance of how this issue arises; similar debates are unfolding in diverse substantive domains. For instance, the pending *Equustek* case in Canada surfaces territorial tensions in the intellectual property and contract context.[11] Across these and other issue areas, the underlying challenge remains the same: when a nation demands a content takedown that goes beyond its physical borders, what is the right outcome?

It may be prudent to take two steps back before answering this question, both because "right" is not a self-defining concept and because a normative solution presented in a vacuum may be too abstracted from realities on the ground. Precisely because the issue is not black and white, it is prudent to chart how this debate is currently unfolding in courts across the globe before prescribing resolutions. The following analysis aims to present just that sort of descriptive picture.

As detailed below, the methodology of this study proceeds in two parts: First, we winnowed a set of cases drawn from the Internet & Jurisdiction (I&J) compilation of content takedown requests[12] and supplemented them with search engine queries to derive a set of recent worldwide, cross-topic cases. At times, these search engine queries led us to closely related findings, such as associated lower court precedent, appellate court decisions, or substantively overlapping cases; when we located such cases, we included them in our analysis. However, we did not actively seek out materials beyond the I&J compilation. We placed cases (as defined below in Part 2.2) into a taxonomy that juxtaposes the

---

Regardless of the policy merits of any such choices, especially when a voluntary agreement of this sort evolves after conversations with government stakeholders, such self-regulatory measures may help companies to maintain a strong presence in that country or region.

[11] Equustek Solutions Inc. v. Google Inc., 2015 BCCA 265 (Can.). The Supreme Court of Canada heard arguments in December 2016. For an overview of the lower court's decision, see Equustek Solutions Inc. v. Jack, Colum. Univ. Glob. Freedom of Expression, https://globalfreedomofexpression.columbia.edu/cases/equustek-solutions-inc-v-jack-2/ (last visited Mar. 5, 2017).

[12] I&J Retrospect Database, Internet & Jurisdiction, http://www.internetjurisdiction.net/publications/retrospect (last visited Mar. 9, 2017).

amount of substantive legal consensus regarding a particular category of cases (*e.g.*, intellectual property, pornography, defamation, etc.) against the intended geographic scope (local, regional, or global) of the court order in that case.[13] The hope is that visualizing cases in this way reveals what the global legal terrain currently *is*, setting the stage for an ongoing dialogue about what the underlying principles *should be* — and how to develop legal principles and policy measures that can help to bridge any gaps.

2. THE FIRST ACT: DEFINING THE STUDY

2.1. Casting the Scope of the Analysis

This study does not aspire to cover all worldwide content takedown requests, no matter their source or form. In our research, the unit of analysis is a single case, defined as an individual content takedown request drawn from the I&J Retrospect.[14] To focus the analysis, we also limit the temporal scope of the study to include only disputes resolved between January 2014 and February 2017.

Future research might augment this work by expanding the years under review and / or by including case studies compiled from other sources. For now, in the interest of canvassing the terrain in a comprehensive and administrable way, we draw from the I&J corpus and define a case in a way that is substantively broad and procedurally narrow: a case can arise in any domain, and can be brought by an individual, organization, or governmental authority in any jurisdiction, yet the content takedown request must be resolved in an administrative or judicial proceeding. Put differently, regardless of who brings a case or where it arises, the content takedown request must occur via a formal, regularized, and transparent legal process.

We implement this methodology in order to engage in a more precise assessment of how courts and related components of nation–states' legal systems are currently resolving jurisdictional issues as a matter of law. We are nonetheless cognizant of what this framing excludes. For instance, our study does not account for takedown requests within regimes that lack structured and consistent legal processes. It thus excludes national mechanisms, such as China's "Great Firewall," that permit wholesale censorship or broad filtering of internet content;

---

[13] For more detail on this taxonomy, see *supra* at Part 3.

[14] I&J Retrospect Database, Internet & Jurisdiction, http://www.internetjurisdiction.net/publications/retrospect (last visited Mar. 9, 2017). As noted previously, we used internet searches based on the I&J descriptions to learn more about the relevant cases.

relatedly, it excludes authoritarian, autocratic, or dictatorial nation–states, such as North Korea, that tend to regulate by executive order without oversight by other branches of government. And across all systems of government, democratic or not, our study does not encompass takedowns that occur in other ways, ranging from extra-judicial mechanisms, such as a direct police order or an executive order;[15] to cross-jurisdictional requests, such as country A demanding that country B order an ISP to block all domain names associated with a known copyright infringer; to industry self-regulation, whether wholly voluntary or in anticipation of a more formal government request.

In drawing lines in this way, we by no means intend to downplay the importance of the excluded issues, but rather to suggest that they may be conceptualized as distinct from our analysis of how administrative and judicial adjudicators are treating content takedown requests in the internet era. Again, we begin the conversation at this point with the goal of catalyzing more discussion and research, rather than in an effort to present an exhaustive categorization.

2.2. Arranging the Research Corpus

To ensure consistency in the analysis, we collected, to the best of our ability based on publicly available data, a common set of factors across all cases. Recognizing how quickly change is occurring in this domain, we limited the dataset to the I&J Retrospect's listings from January 2014 to February 2017. As described above, we used internet searches to gather more details about these cases, which led us to discover a small number of closely associated cases that we added to the core I&J dataset. We manually reviewed these listings and, for each case that involved a formal takedown request along the lines articulated in Part 2.1 above, documented the following items:

- Name of Case
- Cause of Action: What claim is made to justify the request?
- Parties Involved
- Who is making the complaint?
- Who is the target of the takedown request?
- Speaker (if the original speaker is not a party to the case)
- Outcome (including scope of any takedown order)

---

[15] Note that such orders may be particularly prevalent as a way for less democratic nations to block opposition voices during periods of political protest or during elections. Consider, for example, Myanmar's blockage of several sites during protests or elections to "preserve national order." *See* Jilian C. York, *Myanmar's Facebook Block Could Signal More to Come*, EFF (July 14, 2014), https://www.eff.org/deeplinks/2014/07/myanmars-facebook-block-could-signal-more-come.

In some instances, we were not able to ascertain these facts from either descriptions of the case or from the text of the decision. Some cases, for example, might fail to specify whether the party making a complaint was an individual with territorial links to the nation in which the case was adjudicated. In other cases, a court might not explain the intended scope of the takedown order in much, or any, detail. In these cases and in other instances where information was not available, we adopted the following set of rebuttable presumptions and practices:

- If the nationality/residence of the person or entity bringing a case was not clear, we applied traditional principles of territoriality and assumed that this party was a citizen or resident of the nation in which the case was brought.
- If we could not ascertain the location of an intermediary or individual at whom a takedown request was targeted, we again applied traditional principles of territoriality and assumed that party was located in the country in which the case was brought. We did not undertake additional research to confirm factors such as the physical location of assets (*e.g.*, servers), an individual's residence, or an entity's principal place of business.

In a small number of cases, we could not confirm the status of adjudication, and consequently cannot be certain whether a case was appealed or resulted in a final resolution in or out of the courts. The information included in our taxonomy reflects our best efforts to reflect the state of play as of March 21, 2017.

3. THE SECOND ACT: CATALOGING AND ARRANGING CASES

The heart of the analysis lies in our taxonomy, which places the selected set of I&J cases along an X- and Y-axis.

The **X-axis** refers to the geographic scope of the order by the court, assessing whether the takedown order's intended territorial reach is:

- **Local** (*e.g.*, confined to national territorial borders);
- **Regional** (*e.g.*, tied to a cross-national entity, such as the European Union (EU)); or
- **Global** (*e.g.*, applicable to every publication of a given piece of content, across the world).

The **Y-axis** reflects the degree of substantive consensus around an issue, arraying cases according to how much nation–states diverge with regard to their treatment of that kind of content. We assess cases on a spectrum:

- **High Substantive Consensus:** Little or no cross-border variation on policy outcomes, given high legal consensus that a particular category of content should always be taken down or blocked. A prominent example is the general, albeit tacit, transnational agreement that child pornography should be removed, regardless of the jurisdiction in which it appears. Put slightly differently, this category consists of content that "thou shalt not" post or host, given contemporary international understandings in all or most jurisdictions.
- **Mixed Cases:** Variation between jurisdictions regarding the proper disposition of a case that involves that category of content, depending on national policy. In such an instance, country A might consider the content to be inconsistent with its laws and/or regulations, and country B might have no such restriction. The key point is that, so long as there is no extraterritorial application of the relevant laws, these positions are reconcilable. For instance, country A might ban defamatory comments regarding private figures, and allow citizens to sue to prevent the publication of that content in country A, whereas country B might permit — but does not affirmatively require — publication of that same content. We conceptualize this set of cases as instances in which the laws or regulations of one country prescribe, "thou shalt not," and another country provides, "thou canst."
- **Conflicting Positions:** Irreconcilable conflicts of law, in which a content takedown requirement in one jurisdiction fundamentally clashes with the content publication requirement in another jurisdiction. For example, a court in a European country in which the RTBF applies might require a search engine to remove listings associated with an old criminal offense, whereas another country's laws may demand publication of the photos of criminal offenders, such that this content could not be removed without contravening this requirement. These cases may be rare — indeed, our analysis failed to locate any examples of this category. We nonetheless include this conceptual space in our taxonomy, on the theory that such instances in which one nation demands "thou shalt

not" and another demands "thou shalt" represent important pressure points in the current global legal regime.[16]

Within each X/Y intersection, we clustered cases according to the issue area involved, with cases grouped by country within a particular cluster. We adopted the following substantive groupings: Intellectual Property[17]; Pornography/Prostitution[18]; Defamation/Privacy[19]; Blasphemy[20]; Hate Speech/Terrorism/Extremism[21]; Right to Be Forgotten (RTBF)[22]; and Compliance with National Laws.[23]

Throughout the document, to account for cases in which there might be a territorial impact that is distinct from the intended scope of the order, we colored cases as follows:

---

[16] It is worth underscoring that we observed hard conflicts of law that fell just outside the scope of this study, given its focus on *content* takedowns. Notably, there appear to be hard conflicts of the sort described here with regard to disclosure of user data. For example, in one recent case, the Indian Madras High Court ordered a U.S.-based search engine (Google) and its subsidiary (YouTube) to disclose details about a user who posted a YouTube video that an Indian company flagged as defamatory. Complying with a previous ruling from the same court, YouTube blocked access to the video on the Indian version of the platform on the ground that it defamed a private company, but YouTube refused to divulge the content poster's identity. The platform argued that the IP address resolves outside of the Indian jurisdiction, and stressed that complying with the order would expose it to legal action under American law. In other words, a hard clash of law occurred insofar as Indian law told the company that it must disclose the user's identity, but American law told the company that it could not do so. *See* Prachi Shrivastava, *Fox Mandal wins for Lebara Foundation in Madras HC, against Poovayya for Google, YouTube*, Legally India (Oct. 27, 2016, 5:28 PM), http://www.legallyindia.com/litigation/fox-mandal-wins-for-lebara-foundation-in-madras-hc-against-poovayya-for-google-youtube. This case is included as case 3-10. India—YouTube defamation in the taxonomy below.

[17] Any intellectual property case, including copyright or trademark. Note, however, that the preponderance of cases are copyright suits that involve piracy allegations.

[18] Any case involving pornographic content, including child pornography and revenge porn, or other forms of prurient content.

[19] Any case involving a cause of action centered on the harm to an individual's personality, reputation, or right to control personal information (*e.g.*, privacy rights).

[20] Any case involving an insult to a religion, to any member of that religion, or to any of its central tenets.

[21] Any case involving speech alleged to threaten an individual due to their membership in a particular class or because of particular attributes they possess, or speech alleged to incite violence or otherwise threaten national security.

[22] Any case involving a request to delist content about an individual, whether or not it conforms to the European requirements that the information be "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes."

[23] Any case involving an allegation of non-compliance with a particular national law that is not clearly encompassed by another category.

- Purple text indicates a potential unintended extraterritorial impact/effects in implementation of the order.
- Green text indicates a definite unintended extraterritorial impact/effects in implementation of the order.

Significantly, our coding of cases and our placement within the taxonomy reflects the final outcome of the case, as opposed to what the impact might have been had the case come out another way. For instance, where the resolution of the case resulted in no change to the status quo (*e.g.*, the party bringing a suit lost its challenge, and content was left unaltered), we do not account for the potential or actual territorial or extraterritorial effects had the case come out differently.

Our categorization according to this schema follows, accompanied by a cross-referenced table that separately lists the cases by issue area for ease of reference. In this table, we include a brief synopsis of the holding in each case, along with especially pertinent information about that case.

Degree of Substantive Legal Consensus

High Substantive Consensus

Intended Territorial Scope of Takedown Order

Local	Regional	Global
Intellectual Property	Intellectual Property	Intellectual Property
1-1. Spain—Telcinco v. YouTube	(None included in set)	1-24. Canada—Equustek v. Google
1-2. Spain—Goear		1-25. U.S./Hong Kong—MegaUpload
1-3. Spain—Pirate Bay		
1-4 U.K.—Streaming sites		
1-5. U.K.—Popcorn Time		
1-6. U.K.—Pirate Bay		
1-7. Italy—Filmakerz.org		
1-8. Italy—24 websites blocked		
1-9. Germany—GEMA		
1-10. Germany—OLG		
1-11. Germany—Key Systems		
1-12. Austria—Pirate websites		
1-13. Austria—Pirate Bay		
1-14. Iceland—Pirate Bay		
1-15. France—Pirate Bay		
1-16. The Netherlands—Pirate Bay		
1-17. Denmark—Voga.com		
1-18. Russia—TracksFlow v. Warner Bros.		
1-19. Israel—Popcorn Time		
1-20. U.S.—Kickass Torrents		
1-21. U.S.—Elf Man		
1-22. U.S.—Innocence of Muslims		
1-23. Argentina—Pirate Bay		

Purple: Potential unintended extraterritorial impact/effects in implementation

Green: Definite unintended extraterritorial impact/effects in implementation

Degree of Substantive Legal Consensus

Mixed Cases

Intended Territorial Scope of Takedown Order

Local	**Regional**	**Global**
<u>Pornography/Prostitution</u>	<u>Pornography/Prostitution</u>	<u>Pornography/Prostitution</u>
2-1. U.K.—Irish "shame page" 2-2. Germany—Revenge porn 2-3. U.S.—Revenge porn 2-4. U.S.—Backpage.com 2-5. Argentina—Model's thumbnail images 2-6. Russia—Pornography 2-7. Egypt—Prostitution on Facebook 2-8. Pakistan—Pornography	(None included in set)	(None included in set)
<u>Defamation/Privacy</u>	<u>Defamation/Privacy</u>	<u>Defamation/Privacy</u>
3-1. Germany—Mosley Orgy 3-2. Germany— "Merkel selfie" 3-3. U.K.—PJS v. News Group Newspapers Ltd. 3-4. Ireland—Facebook/Djibouti 3.5. Ireland—Petroceltic 3-6. Brazil—Dafra 3-7. Brazil—Political defamation 3-8. Turkey—Ministerial corruption scandal 3-9. Turkey—Twitter and YouTube 3-10. India—YouTube defamation	3-11. Hong Kong—Investor	3-12. Japan—Negative Reviews

Degree of Substantive Legal Consensus

Hard Clash of Laws

Intended Territorial Scope of Takedown Order

Local	**Regional**	**Global**
Blasphemy	Blasphemy	Blasphemy
4-1. Pakistan—Innocence of Muslims	(None included in set)	(None included in set)
Hate Speech/Terrorism/Extremism	Hate Speech/Terrorism/Extremism	Hate Speech/Terrorism/Extremism
5-1. U.S.—Jordanian ISIS victims 5-2. India—Religious hate speech	(None included in set)	(None included in set)
Right to be Forgotten (RTBF)	Right to be Forgotten (RTBF)	Right to be Forgotten
6-1. Spain/EU—Costeja 6-2. Spain—De-indexation delay 6-3. Colombia—RTBF 6-4. Brazil—RTBF 6-5. Chile—RTBF 6-6. Mexico—RTBF 6-7. India—False marriage certificate 6-8. Japan—Criminal records 6-9. Japan—Child prostitution charges 6-10. China—RTBF 6-11. Hong Kong—Matrimonial documents	(None included in set)	6-12. Hong Kong—Right to be deindexed
Compliance with National Laws	Compliance with National Laws	Compliance with National Laws
7-1. Brazil—*Secret* App 7-2. India—Prenatal Gender Testing & Abortion 7-3. Russia—Suicide 7-4. Russia—Homosexuality	(None included in set)	(None included in set)

I. High Substantive Consensus

Intellectual Property

1-1. Spain—Telcinco v. YouTube: Appellate court applying European law found YouTube not liable for copyright violations in user-generated content available on its .com and .es versions.

1-2. Spain—Goear: Court of first instance (Audiencia Nacional) ordered ISPs to block unlicensed music streaming site Goear.com.

1-3. Spain—Pirate Bay: Court of first instance issued injunction requiring local ISPs to block file-sharing site Pirate Bay within 72 hours.

1-4. U.K.—Streaming sites: Court of first instance (Madrid Central Administrative Litigation Court No. 5) ordered six British ISPs to block access to four websites (Megashare, Viooz, Watch32, and Zmovie) that either directly stream or provide links to illegal streams of copyrighted movies.

1-5. U.K.—Popcorn Time: Court of first instance (High Court) ordered British ISPs to block access to Popcorn Time, a media player that streams content from file-sharing websites.

1-6. U.K.—Pirate Bay: Court of first instance (High Court) ordered several major U.K. ISPs to block access to Pirate Bay and its proxies around the world.

1-7. Italy—Filmakerz.org: Appellate court (Rome Court of Appeals) overturned a lower court order blocking the Filmakerz.org video streaming site in its entirety, finding it to be overbroad.

1-8. Italy—24 websites blocked: Court of first instance (Tribunal of Rome) ordered Italian ISPs to block access to 24 websites (including Mega, MegaUpload, and Mail.ru, Russia's fifth most popular website) based on Italian producer's complaint about unauthorized distribution of two movies. Appellate court later reversed the blocking order for sites that appealed as disproportionate.

1-9. Germany—GEMA: Germany's highest non-constitutional court (Federal Court of Justice) upheld ruling requiring ISPs to block access to copyright-infringing websites with unidentifiable hosts and operators, though only as a last resort and if reasonable under the circumstances.

1-10. Germany—OLG: Appellate court (Higher Regional Court of Celle) held that recipients of cease and desist injunctions shall "ensure by appropriate measures" that infringing content cannot be accessed, including via search engine results. The scope of the latter requirement is unclear, but at a minimum, requires a person subject to the injunction to "provide Google with a request for deletion in the Google cache or removal of the contents already deleted by the website."

1-11. Germany—Key Systems case: Court of first instance (Regional Court of Saarbrücken) ordered registrar to delete the DNS entry of a foreign website that systematically violated copyright (in this case, by illegally streaming music), finding the registrar liable for that site's copyright infringement because specific allegations made it "obvious" that the site was used primarily for copyright infringement.

1-12. Austria—Pirate websites: In a case referred by the Austrian Supreme Court, the European Court of Justice held that ISPs can be ordered to block access to websites that contain copyright-infringing content, so long as orders are proportionate and balance copyright with fundamental rights. However, the block was lifted in May 2016.

1-13. Austria—Pirate Bay: Court of first instance (Vienna Commercial Court) ordered an ISP to block access to Pirate Bay.

1-14. Iceland—Pirate Bay: Court of first instance (Reykjavík District Court) ordered Icelandic ISPs to block access to file-sharing sites Pirate Bay and Deildu.

1-15. France—Pirate Bay: Appellate court (Paris High Court) ordered four major ISPs to block access to Pirate Bay and associated mirror and redirection sites.

1-16. The Netherlands—Pirate Bay: Appellate court (The Hague Court of Appeal) struck down a court of first instance order requiring two ISPs to block Pirate Bay, finding the court of first instance's determination "inefficient" and "disproportionate."

1-17. Denmark—Voga.com: Danish court of first instance ordered Voga.com, an Irish website that sells replicas of Danish furniture, to prevent visitors with a Danish IP address from accessing the site.

1-18. Russia—TracksFlow v. Warner Bros: Unspecified Russian court ordered the termination of the domain name of a site that plays music sourced from third-

party sites (*e.g.*, YouTube) without the permission of copyright owners. Since the domain name was registered through a U.S.-based registrar, the enforceability of the order is uncertain.

1-19. Israel—Popcorn Time: Appellate court (Tel Aviv District Tribunal) reversed injunction requiring ISPs to block Popcorn Time.

1-20. U.S.—Kickass Torrents. Federal court of first instance (D. Ill.) ordered the seizure of domain names and bank accounts belonging to Kickass Torrents, an illegal file-sharing site owned by a Ukrainian national.

1-21. U.S.—Elf Man: Federal court of first instance (D. Wash.) dismissed copyright infringement lawsuits filed by the makers of the movie *Elf Man* against hundreds of individuals whose IP addresses were linked to illegal downloads of the film, since "simply identifying the account holder associated with an IP address tells us very little about who actually downloaded 'Elf Man' using that IP address."

1-22. U.S.—Innocence of Muslims: Federal appellate court (9th Cir.) initially ordered Google to remove *The Innocence of Muslims* film over a copyright claim by an actor, but the court later reconsidered and reversed its earlier ruling.

1-23. Argentina—Pirate Bay: Federal court of first instance ordered eleven ISPs to block Pirate Bay for systematically violating copyright. The order has the effect of preventing certain internet users in Paraguay from accessing Pirate Bay, since traffic from that region is routed through Argentinian ISPs.

1-24. Canada—Equustek v. Google: Appellate court (B.C. Court of Appeal) upheld an injunction issued by a court of first instance requiring Google to de-index, on a global basis, a site selling pirated goods. The Supreme Court of Canada has heard Google's appeal and a decision is pending.

1-25. U.S./Hong Kong—MegaUpload: Federal court of first instance (E.D. Va.) issued an order authorizing the FBI to seize the domain name of Hong Kong-based file-sharing platform MegaUpload after the site and its executives were charged with criminal copyright infringement. Pursuant to a request from the U.S., the authorities in Hong Kong froze the company's assets.

II. Mixed Cases

Pornography/Prostitution

2-1. U.K.—Irish "shame page": Court of first instance (Belfast High Court) refused to dismiss a case filed against Facebook by a 14-year old girl whose nude picture was repeatedly published on a Facebook "shame page" and used to blackmail her.

2-2. Germany—Revenge porn: Court of first instance ordered defendant, who was previously in a relationship with the plaintiff, to delete consensual nude photos the defendant possessed of the plaintiff. The plaintiff had requested their deletion; the defendant refused yet showed no intention of publishing or distributing the photos.

2-3. U.S.—Revenge porn: State appellate court (Texas) ruled that under § 230 of the Communications Decency Act, a hosting provider is not liable for "revenge porn" published by a website it hosts.

2.4. U.S.—Backpage.com: Federal appellate court (1st Cir.) held that Backpage.com, a classified ad service, could not be held liable for its platform's alleged role in facilitating prostitution and sex trafficking, despite evidence that the site "knowingly concealed" evidence of such activity. U.S. Supreme Court denied certiorari.

2-5. Argentina—Model's thumbnail images: In a case brought by a model who sought to block Google from displaying thumbnails of her images and bar Yahoo and Google from returning pornographic material on searches of her name, the Supreme Court (1) treated the thumbnails as links rather that Google's own content; (2) rejected any prospective obligation to filter or block infringing content; and (3) held that search engines should be liable for the content they provide only insofar as they have actual knowledge of their harmful nature, or are grossly negligent.

2-6. Russia—Pornography: Acting through two court orders, Russia's communications regulator (Roskomnadzor) ordered ISPs to indefinitely block access to two pornographic websites (Pornhub and YouPorn), but later cancelled the order.

2-7. Egypt—Prostitution on Facebook: Administrative court ruled against claimant seeking to block Facebook in Egypt on grounds that it "facilitates prostitution and

propagates false information," holding that problematic pages should be dealt with individually.

2-8. Pakistan—Pornography: Pursuant to a Supreme Court ruling commanding the Pakistan Telecommunication Authority (PTA) to "take remedial steps to quantify the nefarious phenomenon of obscenity and pornography" in the country, the PTA ordered ISPs to block over 400,000 websites believed to host pornography.

Defamation/Privacy

3-1. Germany/France—Mosley orgy: German court of first instance ordered Google to de-index six pictures of former Formula 1 boss Max Mosley participating in a Nazi-themed sadomasochistic orgy from its German website. (Separately, in November 2013, a French appellate court (Paris Superior Court) ordered Google to block the images in France.) This dispute is related to a 2008 matter decided by an English appellate court and an associated 2011 ECHR case, which determined damages but did not address content removal.

3-2. Germany— "Merkel selfie:" Court of first instance refused to order Facebook to proactively vet and remove posts falsely accusing a man of criminal behavior and featuring a "selfie" he took with German Chancellor Angela Merkel in 2015.

3-3. U.K.—PJS v. News Group Newspapers Ltd: U.K. Supreme Court upheld an injunction barring the disclosure of a celebrity's identity or sexual affairs in England and Wales, even though the information was public in other jurisdictions (including Scotland).

3-4. Ireland—Facebook/Djibouti: Court of first instance rejected application by Djibouti's President to require Facebook Ireland to remove defamatory material and suspend the accounts responsible for their publication.

3.5. Ireland—Petroceltic: Court of first instance (Dublin High Court) ordered U.S.-based Auttomatic's Irish subsidiary (Aut O'Mattic A8C Ireland Ltd.) to remove from its Wordpress.com service, allegedly defamatory material posted by a third-party user about an Irish-based energy exploration company.

3-6. Brazil—Dafra: Brazil's highest non-constitutional court (Superior Tribunal of Justice) upheld injunction requiring Google to remove from YouTube versions of video advertisements for a motorcycle company (Dafra) that users had dubbed with messages that critiqued or lampooned the company. The injunction covers any "unauthorized" content.

3-7. Brazil—Political defamation: Court of first instance ordered a nationwide, 24-hour block against Facebook for its failure to comply with an injunction requiring it to block content that allegedly defamed a mayoral candidate. Facebook complied with the injunction before the National Telecommunications Agency (Anatel) could implement the block.

3-8. Turkey—Ministerial corruption scandal: A court of first instance in Ankara barred the Turkish government from blocking Twitter for refusing to comply with the Turkish telecommunications authority's order requiring the takedown of content accusing a former minister of corruption.

3-9. Turkey—Twitter and YouTube: Turkey's Constitutional Court struck down the government's nationwide ban on Twitter, which had been enacted after the publication of tweets accusing then-Prime Minister Erdogan of corruption. A court of first instance in Ankara subsequently cited this Twitter ruling, narrowing a similar national ban on YouTube to apply only to 15 accounts that were used to publish leaked videos of a secret military conversation.

3-10. India—YouTube defamation: Appellate court (Madras High Court) ordered U.S.-based company (Google Inc.) and its subsidiary (YouTube) to block a video flagged as defamatory in the Indian version of the platform. Google moved a single judge for modification of the order to clarify that the video couldn't be blocked outside India. The Court also requested the foreign IP address of the user that published the content, but Google refused to divulge the user's identity, since complying with the order would expose Google to legal action under U.S. law.

3-11. Hong Kong—Investor. Court of first instance ruled that a Hong Kong-based investor could sue Google for defamation when search results portray him as a murderer and pedophile. Google's appeal is pending.

3-12. Japan—Negative reviews: Court of first instance in Chiba ordered Google to de-index, on a global basis, search results that turn up negative reviews of a doctor who has sworn an affidavit claiming they are false. Google has stated an intention to appeal.

Blasphemy

4-1. Pakistan—Innocence of Muslims: Supreme Court of Pakistan ordered a nationwide block of YouTube after it refused to remove *The Innocence of Muslims.* However, after Pakistani NGO "Bytes for All" appealed the ban on grounds that it was disproportionate, an appellate court (High Court of Lahore) agreed that warning pages could instead be displayed on YouTube before controversial videos in the Pakistani jurisdiction, and permitted the restoration of access to YouTube.

Hate Speech/Terrorism/Extremism

5-1. U.S.—Jordanian ISIS Victims: Federal court of first instance (N.D. Cal.) granted Twitter's motion to dismiss a lawsuit filed by next-of-kin of two Americans killed by ISIS, claiming the social media platform provides "material support" to the terrorist group.

5-2. India—Religious hate speech: A court of first instance in Delhi ordered six sites (including Facebook, Google, YouTube, and Blogspot) to remove videos and links containing religious hate speech that disparaged Islam and affecting national social integration, giving the companies two weeks to present further plans for policing their networks.

Right to be Forgotten (RTBF)

6-1. Spain/EU—Costeja Case: European Court of Justice ruled that individuals have a statutory right to request the de-indexation of search engine results linked to their name that are "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed."

6-2. Spain—De-Indexation delay: Appellate court (Barcelona Court of Appeals) ordered Google Spain to pay damages for taking ten months to comply with an order from the country's Data Protection Authority ordering the de-indexing of results pertaining to an old drug conviction.

6-3. Colombia—RTBF: Constitutional Court rejected a RTBF-style request for removal of information, instead ordering a newspaper to update true yet outdated information and use technological tools to ensure that a search based on the plaintiff's name would not lead to the disputed content. All claims against Google were dismissed.

6-4. Brazil—RTBF: Brazil's highest non-constitutional court (Superior Tribunal of Justice) refused to recognize a right to have content de-indexed by search engines.

6-5. Chile—RTBF: The Chilean Supreme Court ordered a news website to delete an article concerning on a man's decade-old conviction for child molestation, on the basis that the continued availability of the article affected his work prospects and life in the community.

6-6. Mexico—RTBF: Federal Commission on Personal Data granted businessman's request to have Google remove search results that cast his family's business dealings in a negative light, finding that the country's privacy law allowed lawfully published articles to be removed from search results when "persistence causes injury."

6-7. India—False marriage certificate: Appellate court (Karnataka High Court) granted a father's petition to de-index search results pertaining to a false marriage certificate bearing his daughter's name and related litigation, in view of the reputational harm she would suffer from the accessibility of these results. The court also granted an associated petition to remove the daughter's name from the digital records maintained by the court.

6-8. Japan—Criminal records: Court of first instance (Tokyo District Court) ordered Google to de-index 120 of 230 search results that discussed the applicant's criminal record.

6-9. Japan—Child prostitution charges: Japan's Supreme Court dismissed a man's request to have Google de-index references to his arrest on child pornography charges, holding that the "public's right to know outweighed the man's right to privacy, given the serious nature of his crimes." The Supreme Court laid out additional criteria for the adjudication of de-indexation requests pursuant to Japanese data protection laws.

6-10. China—RTBF: A court in Beijing rejected RTBF-style claim against Baidu after a man requested that all personal information relating him to a former employer be de-indexed from the search engines.

6-11. Hong Kong—Matrimonial Documents: Hong Kong Privacy Commissioner ordered the owner of a Hong Kong corporate governance information website that provides pubic access to court judgments to delete some documents related to a matrimonial case. The case is currently on appeal.

6-12. Hong Kong—Right to be De-indexed: Court of first instance admitted a suit of a local entertainment tycoon against Google Inc. for autocomplete suggestions on Google Search that allegedly damage his reputation. The judge cited the ECJ *Costeja* decision as well as the Canadian *Equustek* decision to delete search results globally.

Compliance with National Laws

7-1. Brazil—Secret App: Court of first instance (Fifth Civil Court of Victoria) issued a preliminary injunction to remove the *Secret* app from Google and Apple stores in the Brazilian jurisdiction and to delete copies of the software on Brazilian smartphones via remote mechanisms, since anonymity is proscribed in the country.

7.2- India—Prenatal gender testing & abortion: Supreme Court of India ordered Google, Yahoo, and Microsoft to apply the "doctrine of auto-block" (sic.) and proactively prevent users from obtaining any results for searchers on 22 keywords pertaining to prenatal gender testing and sex selective abortion, both of which are illegal in the country. The Court also authorized an agreement between the Indian Ministry of Health and the IT companies.

7-3. Russia—Suicide: Russian telecommunications regulator Roskomnadzor blocked Github after it failed to comply with government requests to take down pages satirically discussing suicide. Since GitHub uses HTTPS, ISPs were forced to block the entire Github site, rather than merely blocking access to the offending blog. The order was lifted after GitHub began geoblocking such content in Russian territory.

7-4. Russia—Homosexuality. Court of first instance in Siberia ordered nation-wide blocking of the popular LGBT news website BlueSystem.ru, without notice or explanation.

III. Hard Clash of Laws

(None included in set)

4. FINDINGS

Below, we offer preliminary reflections on our research, with an eye to highlighting high-level patterns in the observed cases. As noted previously, we by and large refrain from overarching conclusions and intend for our descriptions to stand on their own terms. We hope that our taxonomy and descriptions will stimulate further discussion regarding how territorial presumptions should or should not be applied to the online space. We also recommend further research, including not only potential expansions of the dataset we used and the time periods we studied, but also further examination and analysis of cases to test the robustness of our core findings.

Taking the dataset as a whole, our primary observation is that most of the content takedowns — whether operationalized through wholesale removal, de-indexing, or blockages — accord with territorial principles. Put simply, regardless of the substantive degree of consensus (our Y-axis), extraterritorial takedowns of content (*e.g.*, takedown orders intended to affect a regional or global removal of content, as depicted on our X-axis), are rare. Even when accounting for the potential or definite *unintended* extraterritorial impact of an order (which we depict, respectively, in purple and green), the cases with an extraterritorial impact are few and far between.

Examining our substantive issue areas in more detail puts our core finding — that at least for the time being, most content takedown orders respect the principle of territoriality — into stark relief. Below, we focus on our intellectual property cases, which are especially illustrative of this general point.

4.1. Deep Dive: Intellectual Property & Territoriality

We focus on intellectual property cases because they represent the largest portion of our sample.

As depicted in the table on the next page, the preponderance of our cases are intellectual property disputes (25 of 64, or 39%). Within the intellectual property cluster, all but one of the cases that we identified involved copyright takedown requests, and most of these cases conformed with territorial principles (*e.g.*, any takedown required only local removal within the territorial jurisdiction of the court and did not carry any unintended extraterritorial effects). The sole exception, a trademark case (case 1-24[24]), is doubly anomalous given the global (and hence extraterritorial) scope of the court's order. Already, however, courts

[24] Canada—Equustek v. Google.

in other jurisdictions have begun to cite *Equustek* in support of orders with potentially extraterritorial scope (cases 3-12, 6-12[25]). Future research might assess the degree to which evolving precedent builds from anomalous cases, rather than continuing compliance with the territorial principles that seem to apply in the majority of cases.

Summary Table of Cases

Substantive Area	No. of Cases	% of Total[26]
Intellectual Property	25	39%
Pornography/Prostitution	8	13%
Defamation/Privacy	12	19%
Blasphemy	1	2%
Hate Speech/Terrorism/Extremism	2	3%
Right to be Forgotten	12	19%
Compliance with National Laws	12	6%

Substantively, the majority of these copyright cases are piracy claims directed to file-sharing and "torrent" sites such as the Pirate Bay and MegaUpload (cases 1-3, 1-6, 1-13, 1-14, 1-15[27]). At least within our dataset, most jurisdictions appear to distinguish between file-sharing sites and streaming sites such as YouTube and hold such file-sharing sites liable for copyright-infringing third party content. Accordingly, courts adjudicating such claims ordered the immediate takedown of the allegedly infringing content or, in extreme cases, the wholesale blocking of the sites (cases 1-2, 1-3, 1-9, 1-11, 1-13, 1-14, 1-15,1-18, 1-23[28]). On balance, courts seem generally to find blocking disproportionate or excessive unless there is a high degree of substantive consensus on the illicit nature of the underlying act, as appears to be the case in piracy cases (cases 1-7, 1-8, 1-9, 1-12, 1-16, 1-19, 1-21, 2-7, 3-8 3-9[29]).

These findings suggest a high level of international consensus for content takedown orders that involve intellectual property. Notably, most of the copyright cases that we studied were adjudicated in OECD

[25] 3-12. Japan—Negative Reviews, 6-12, Hong Kong—Right to be deindexed.

[26] Percentages do not add up to 100% due to rounding.

[27] 1-3. Spain—Pirate Bay, 1-6. U.K.—Pirate Bay, 1-13. Austria—Pirate Bay, 1-14. Iceland—Pirate Bay, 1-15. France—Pirate Bay.

[28] 1-2. Spain—Goear, 1-3. Spain—Pirate Bay, 1-9. Germany—GEMA, 1-11, Germany—Key Systems, 1-13. Austria—Pirate Bay, 1-14, Iceland—Pirate Bay, 1-15, France—Pirate Bay, 1-18. Russia—TracksFlow v. Warner Bros, 1-23. Argentina—Pirate Bay.

[29] 1-7. Italy—Filmakerz.org, 1-8. Italy—24 websites blocked, 1-9. Germany—GEMA, 1-12. Austria—Pirate websites, 1-16. The Netherlands—Pirate Bay, 1-19. Israel—Popcorn Time, 1-21. U.S.—Elf Man, 2-7. Egypt—Prostitution on Facebook, 3-8. Turkey—Ministerial corruption scandal, 3-9. Turkey—Twitter and YouTube.

countries, and future research might assess whether this trend is equally strong across the globe, or whether other patterns emerge.

4.2. Beyond Copyright: Territoriality & Takedown Orders

Even beyond the copyright context, we find that orders to take down, block, or de-index content are generally local, with a small number of regional or global outliers. Indeed, we observed only five cases in which the court order intended a regional or global effect (cases 1-24, 3-12, 6-12[30]) or coordinated with different countries to realize this outcome (cases 1-20, 1-25[31]). Moreover, even when a court order originally intends to have an extraterritorial effect, the ultimate result may not have a global impact (cases 1-18, 3-10[32]).

An important caveat on this trend towards territoriality is the reality of potential unintended extraterritorial effects or definite unintended extraterritorial effects in the implementation of a court's order. Though rare, we did observe potential unintended effects (cases 1-18, 5-1, 6-1[33]) and definite unintended extraterritorial effects (cases 1-20, 1-23, 1-25[34]) in some cases. Despite their rarity, these cases are nonetheless remarkable insofar as they indicate how the decision's effect may reach beyond territorial bounds. In some of these cases, the unintended extraterritorial effects resulted from one jurisdiction's seizure of a website's central servers, such that it could no longer provide services in any other jurisdiction (cases 1-20, 1-25[35]); in others, one country's internet connection relied on another's infrastructure such that a takedown or blockage affected both countries (case 1-23[36]). Future research might take particular care to assess unintended extraterritorial effects, and it might be especially valuable to consider whether and when the legal regime and technological realities of implementation operate at cross-purposes.

However, without discounting the importance of these cases, instances of potential unintended extraterritorial consequences are very much the exception. The trend, if not the rule, is for orders to be enforced and implemented within territorial borders, rather than transposed to the

---

[30] 1-24. Canada—Equustek v. Google, 3-12. Japan—Negative Reviews, 6-12. Hong Kong—Right to be deindexed.

[31] 1-20. U.S.—Kickass Torrents, 1-25. U.S./Hong Kong—MegaUpload.

[32] 1-18. Russia—TracksFlow v. Warner Bros, 3-10, India—YouTube defamation.

33 1-18. Russia—TracksFlow v. Warner Bros, 5-1. U.S.—Jordanian ISIS victims, 6-1. Spain/EU—Costeja.

[34] 1-20. U.S.—Kickass Torrents, 1-23. Argentina—Pirate Bay, 1-25. U.S./Hong Kong—MegaUpload.

[35] 1-20. U.S.—Kickass Torrents, 1-25. U.S./Hong Kong—MegaUpload.

[36] 1-23. Argentina—Pirate Bay.

digital ecosystem in a way that disregards these borders. This pattern holds, even in cases where there is a relatively strong substantive international consensus, such as copyright (which is generally controlled by international treaties) and child pornography (which is generally banned in most jurisdictions), where courts could ostensibly argue that global takedown would reinforce, rather than interfere with, other jurisdictions' regulations.

4.3. The Next Chapter: Research & Future Steps

With the trend towards territoriality in mind, we invite a dialogue that builds from these descriptive findings to take up normative issues. Put simply, if the lines regarding the territoriality and extraterritoriality of court decisions currently appear to be drawn in the way we observe, are these lines the right ones—and what does this conclusion suggest about the role of the legal system? Moreover, future studies might consider whether focusing on formal legal adjudications risks eliding core human rights concerns, including repressive regimes' extra-judicial blockage of information or denial of freedom of expression, in ways that should be taken into account in developing legal or policy prescriptions. We acknowledge that the lines drawn here are merely a start, and look forward to an ongoing conversation about how territorial principles should apply in the internet era.