Stanford Law School | Stanford Center for Internet and Society

Law, Borders, and Speech: Proceedings and Materials

Edited by Daphne Keller

559 Nathan Abbot Way Stanford, CA 94305 cyberlaw.stanford.edu

Law, Borders, and Speech: Proceedings and Materials

Edited by Daphne Keller

Copyright

The Center for Internet and Society

The Center for Internet and Society (CIS) is a public interest technology law and policy program at Stanford Law School and a part of the Law, Science and Technology Program at Stanford Law School. CIS brings together scholars, academics, legislators, students, programmers, security researchers, and scientists to study the interaction of new technologies and the law and to examine how the synergy between the two can either promote or harm public goods like free speech, innovation, privacy, public commons, diversity, and scientific inquiry. CIS strives to improve both technology and law, encouraging decision makers to design both as a means to further democratic values. CIS provides law students and the general public with educational resources and analyses of policy issues arising at the intersection of law, technology and the public interest. CIS also sponsors a range of public events including a speakers series, conferences and workshops. CIS was founded by Lawrence Lessig in 2000. Daphne Keller directs CIS's Intermediary Liability program.

Funding and Disclosures

CIS receives funding through the support of individual and organizational donors, foundation grants, awards of attorney's fees obtained from time to time in connection with its litigation work, cy pres settlements, and the general budget of the law school. A list of current and past donors along with cy pres settlements can be found on our website at https://cyberlaw.stanford.edu/about-us. Facebook Inc. and Google Inc. provided funding specifically for the Law, Borders, and Speech Conference. Neither they nor any other funder directed or otherwise exercised control over the conference or this proceedings volume. Stanford policies provide explicit protection against sponsors who might seek to direct research outcomes or limit the publication of research, and all donors to CIS agree to give their funds as unrestricted gifts.

Daphne Keller was previously Associate General Counsel to Google, and worked on matters including the Canadian *Equustek* and European "Right to Be Forgotten" cases discussed at the conference and in this volume.

Recognition

The conference and this volume would not have been possible without the patience, work, and support of CIS staff and former students, including Amanda Avila, Elaine Adolfo, Luiz Moncau, Riana Pfefferkorn, Al Gidari, Jennifer Granick, Miguel Morachimo, and Ella Hallwass.

Table of Contents

Panels

Appendices

Introduction: Law, Borders, and Speech

The Internet is global. State power and laws usually are not. Online information seeping across borders can reveal human rights abuses to the outside world, help oppressed minorities find allies in other countries, and bring down tyrants. The same unchecked flow of information can undermine the rule of law in democratic countries and help purveyors of dangerous content reach a global audience. Tensions between national law and the Internet's global architecture have existed since the network's earliest days, but become more consequential with each passing year.

David G. Post and David R. Johnson foresaw these issues in their seminal 1996 Stanford Law Review article, *Law and Borders: The Rise of Law in Cyberspace*. The piece was, in Professor Anupam Chander's words, a Helen of Troy among legal publications—the law review article that launched a thousand law review articles. Two decades later, Stanford Law School's Center for Internet and Society convened the Law, Borders, and Speech Conference to reconsider these questions in light of today's more crowded, complex, and contested Internet. It asked experts from around the world to discuss questions about online speech and information, including

- When can one country's laws control speech and access to information around the world? Should some content be universally illegal? Are some legal claims—based on human rights, intellectual property, or data protection, for example—uniquely eligible for cross-border enforcement?

- Could Cyberspace be, as Post and Johnson suggested, 'a distinct "place" for purposes of legal analysis'—de-linked from territorial jurisdiction? If the 'laws' of that 'place' are made by private companies (such as conference sponsors Facebook and Google), what does that mean for national governments and the rule of law?

- Should Internet platforms use technical means to block countries where their services, or information posted by their users, violate national law? Should the answer depend on the country, the technology, or the law at issue?

Conference participants grappling with these questions included company and government representatives, academics, technologists, industry and civil society spokespeople, and more. Speakers came from as far away as Brussels and Argentina, and as close as Twitter and Stanford. One participant called his fellow panelists "the best folks on the subject in the country—or probably the world." Another described the entire audience as a "double black diamond crowd."

A major theme that emerged from the discussion was the power of non-legal forces in shaping online information. Most conspicuously, platforms themselves can act as substitutes for state power—"adjudicating" speech rights under their own Community Guidelines, rather than law. As Emma Llansó and Evelyn Aswad discussed, this expanding corporate power does not necessarily reduce that of government. States that delegate enforcement to platforms can effectively regulate speech by proxy, avoiding constitutional free expression or due process constraints that might otherwise apply. Political pressure from influential nations can have

powerful extraterritorial effect when—as with the European Commission's Code of Conduct for hate speech—platforms agree to "voluntarily" remove content around the world.

Platforms can also act as state proxies when they erect technical barriers, or geoblocks, preventing people in certain countries from accessing forbidden content. David Drummond noted that governments may effectively escape public accountability for their choices by compelling foreign companies to block citizens' access to information—rather than transparently exercising state power and, like China, erecting online barriers themselves. As Joe Hall discussed, though, virtual borders can also become more or less meaningful over time, as the arms race between geoblocking and circumvention technologies progresses.

In other cases, market forces can—for good or ill—lead to unintended consequences for online expression. Small websites' increasing reliance on large-scale web hosting providers like Amazon Web Services may, as Alex Feerst pointed out, effectively concentrate decisions about online expression in the hands of a few companies. Unlike their smaller, local counterparts, multi-national hosting providers may be vulnerable to pressure from numerous governments around the world. At the same time, the power of users can drive important change. As Nicole Wong noted, key questions for platforms in an age of trolling and polarization may concern the demands of users, as much as those of governments. User input and pressure could yet become, in some form, the powerful constitutive force that Post and Johnson envisioned.

A second major conference theme was the misfit between today's speech and jurisdiction problems and the legal tools available to address them. As discussed in one panel, the European "Right to Be Forgotten" illustrates the challenge. Advocates on all sides of that issue see it as fundamentally a question of human rights—the right to privacy, the right to free expression and historical memory, or all of the above in complex balance. For judges, though, it will not be framed in those terms. Courts including the Court of Justice of the European Union are instead asked to resolve highly technical, doctrinal questions about Data Protection law. Data Protection is far from alone in this regard. In one conversation after another, experts found that existing substantive law—on topics from intellectual property to law enforcement data access—provided little clear guidance on cross-border enforcement. A survey of conference participants, asking about interpretations of current law and predictions for the future, identified more points of disagreement than consensus. (See Appendix)

How then to move forward? As a third and perhaps most important theme, participants discussed the tools needed to arrive at wiser outcomes. A top priority is simply more conversation between affected entities. In particular, non-judicial government bodies such as trade, telecommunication, or foreign ministries should join the discussion, as well as technologists, private companies and civil society. Bertrand de la Chapelle described the ongoing work of the Internet and Jurisdiction Policy Network in providing a forum for just such multistakeholder dialog.

Another pressing need is to identify relevant sources of law and develop new analyses to help courts wrangle with questions of online speech and jurisdiction. As Leah Bishop Shaver and Dan Svantesson discussed, attention to the geographic scope of remedies—under existing black letter remedies law or within a court's initial jurisdiction analysis—can provide a starting point.

Human rights law, too, has an important role to play. This is not solely because of the ideals it represents. In the Internet jurisdiction context, human rights law provides a unique and sorely needed starting point of relative consensus and established legal language, already agreed upon by governments around the world. As Paul Schabas discussed, the concept of the "margin of appreciation"—meaning the leeway states have to adopt different, equally permissible, interpretations of rights—may provide some guidance. As Paul argued in a brief for Human Rights Watch, Article 19, and other organizations in Canada's *Equustek* case, this matters for jurisdiction. When countries interpret rights differently within the margin of appreciation—for example, striking different balances between information and privacy rights—human rights doctrine suggests that no country should impose its version on the others.

The Law, Borders, and Speech conference provided a forum for vibrant discussion and cross-pollination among experts working on diverse facets of these issues. This volume attempts to put that lightning in a bottle. It includes a brief summary of each panel, and an Appendix of conference materials, such as hypothetical scenarios discussed at the conference and the results of participant surveys. We hope these materials can be used to expand the conversation begun at the conference, broadening it and sparking new ideas and strategies for the rapidly evolving law of online speech and jurisdiction.

Daphne Keller
Stanford Center for Internet and Society
Director of Intermediary Liability

Big Picture

Summary by David G. Post and David R. Johnson
Watch Video

Panelists:

- Bertrand de la Chapelle - Co-Founder and Director, Internet & Jurisdiction Project
- David R. Johnson - CEO, argumentz.com; Producer, themoosical.com
- Andrew McLaughlin - Medium; Access Now
- David G. Post - Professor of Law (ret.), Temple University Law School; Contributor, Volokh Conspiracy
- Paul Sieminski - General Counsel, Automattic
- Nicole Wong - Senior Advisor, Albright Stonebridge Group

From the Agenda:

> *Which countries' laws and values will govern Internet users' online behavior, including their free expression rights? In 1996, David G. Post and David R. Johnson wrote that "The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply." They proposed that national law must be reconciled with self-regulatory processes emerging from the network itself.*
>
> *Twenty years on, what have we learned? How are we reconciling differences in national laws governing speech, and how should we be reconciling them? What are the responsibilities of Internet speakers and platforms when faced with diverging rules about what online content is legal? And do users have relevant legal rights when their speech, or the information they are seeking, is legal in their own country?*

****

David G. Post, reviewing what the original *Law and Borders* paper got right (and what it got wrong), noted that the central dilemma it had identified—the conflict between an a-territorial global network and an international legal system with territoriality at its core—had certainly proved to be a profoundly challenging one. He suggested that the failure (thus far) to make much headway on these problems of "governance *on* the Internet" (in Bertrand de la Chapelle's phrase)

may be pushing these problems "upward," to the institutions (*e.g.*, ICANN) concerned with "governance *of* the Internet," as they face increasing pressure to leverage their control over critical infrastructure to exercise greater control over online content and conduct.

> ***Institutions like ICANN, concerned with "governance of the Internet," face increasing pressure to leverage their power over critical infrastructure to control online content.***

David R. Johnson suggested that the framework for resolving conflicting claims from multiple sources of rules is to be found in Paul Schiff Berman's work on "cosmopolitan pluralism." All contending jurisdictions should agree to defer to the jurisdiction that has the strongest claim to be the source of decision in a particular case. The strongest claims come from those rule sources—which need not be limited to nation states but which can include online communities—that are "congruent" (*i.e.*, show a high degree of overlap between those affected by the rules and those whose wellbeing was taken into account when making the rules) and which have a viable claim to represent the "consent of the governed." This suggests that online global platforms (like Facebook and Google) would have stronger claims to deference by local law (to their community standards and Terms of Service) if they provided for some form of democratic community oversight.

De la Chappelle observed that the developed legal systems handle the central questions in the administration of law—who sets the rules/norms? to whom do they apply? who adjudicates disputes arising out of them?—remarkably well inside their recognized borders, but that the cross-border nature of Internet interactions subverts that framework, posing the challenge of managing diverse norms in shared online spaces. Unfortunately, the current default relationship among local States seeking to address the problem of conflicting rule-sets is not comity but a form of *non*-cooperation, as States seek to impose their own rules and values on a global basis. He called for the development of protocols for "legal inter-operability," paralleling the technical inter-operability that makes Internet communication possible, and for the formation of multi-stakeholder fora to discuss specific issues and develop solutions that could be adopted by platforms and States on a voluntary basis.

Paul Sieminski asked: What is the role of the platform in all of this? The platform providers (like Auttomatic) have a diverse global user community with its own rules and norms, along with a particular set of values the provider may be seeking to advance (through, among other vehicles, its Terms of Service), while at the same time it has data centers, other assets, and employees in dozens of different countries, each with its own separate legal regime. The platforms thus become targeted choke points in the assertion of local control, but by the same token may have more power than individual users to use legal advocacy as a tool to advance important values, including free expression. Often the big platform companies are the ones fighting the battle—often without much support from their home States—to protect Internet users' rights against overreaching by local sovereigns.

Platforms can become targeted choke points in the assertion of local control, but by the same token may have more power than individual users to advance important values, including free expression.

Nicole Wong noted that the dominant user experience, given the ubiquity of the smart phone and mobile computing, has perhaps shifted from a remote "cyberspace" and is becoming more tethered to physical location. Companies certainly take the efforts of local sovereigns to regulate global platforms into account when deciding where to locate employees and servers and which markets to enter. When large and well-resourced companies take on litigation or policy fights in order to protect their users' rights, the standards they set are often followed by smaller platforms. "When you fight," she said of the large companies, "you raise the defenses for all of us—and when you don't, everyone else retreats." She also suggested that legal/jurisdictional problems posed by global presence may be of less concern to the platform providers than the challenge of accommodating users with diverse values, and that much of the concern these days about content control on the Internet is less about what speech is "legal" and more about what speech is "civil."

Andrew McLaughlin suggested that a significant shift in power on the Internet, from the edge to the core (in the form of the large platforms and cloud storage), has given local sovereigns a lever they can try to use to impose regulatory control. Increasingly, the conflicts faced by tech companies involve differences of law and value between one democratic nation and another (*e.g.*, India has strict rules about comments critical of others' religion), and some countries will attempt to impose rules that others find deeply flawed (*e.g.*, the E.U.'s "Right to Be Forgotten").

****

The ensuing discussion raised a number of additional issues.

One concerned the relationship between private actors and state actors. De la Chappelle observed that cross-border takedown requests create an unusual pairing of State and private parties in resolving complex questions of law and authority. More so than any one government, Internet intermediaries may have a motivation to arrive at harmonized norms or Terms of Service that can function across diverse legal systems. Expanding on the point, McLaughlin observed that the companies may view themselves not merely as commercial actors, but as standing for a set of values and principles. As pointed out by an audience member, however, this increasing public role of private actors does not mean that comity and other doctrines historically governing state-to-state relations should extend to them.

Another concerned the complexity of government powers and motivations: must conflicting interests of different national government institutions—such as security agencies and state departments—be resolved before transnational agreement is possible? When Internet companies refuse to remove content based on national law in a country like Turkey, does this effectively pave the way for more Internet balkanization as governments compel their national ISPs to block content—or entire services—for users in the country?

There also was considerable discussion about geo-location and geo-blocking tools (which served as something of a lead-in to Panel 2, which focused specifically on these technologies): to what extent can their widespread deployment help *solve* the cross-border legal inter-operability problem, allowing content and platform providers to avoid distributing content deemed unlawful in particular territorial jurisdictions, or, conversely, might they impose unjustifiably high costs on the free flow of information that has made the Internet so valuable a global platform?

Geoblocking Tools and the Law

Summary by Graham Smith
Watch Video

Panelists:

- David Drummond - Senior Vice President, Corporate Development, Alphabet
- Mike Godwin - Senior Fellow, R Street Institute
- Joseph Lorenzo Hall - Chief Technologist, Center for Democracy & Technology
- Graham Smith - Partner, Bird & Bird, LLP
- Marketa Trimble - Samuel S. Lionel Professor of Intellectual Property Law, William S. Boyd School of Law, University of Nevada, Las Vegas

From the Agenda:

> *Technical tools can block Internet users from seeing certain content in their countries. How well do they work, what unintended consequences might they have, and is it a good idea for law to pressure private companies to adopt them?*

****

David Drummond introduced the panel. The significance of this panel is that geoblocking tools are in many ways defining and enforcing jurisdiction.

A number of themes emerged from the panel.

What is geoblocking?

The session started with a divergence of definitions. Joseph Lorenzo Hall's technical introduction ranged widely over website and network blocking technologies and described some circumvention tools. Graham Smith distinguished between technical methods used by sites to refuse incoming requests (geoblocking) and techniques to prevent outbound requests reaching their destination (network blocking). Both were discussed extensively during the panel and discussion.

Good, bad or neither?

Marketa Trimble identified two purposes for which tools such as VPN and TOR could be used to circumvent geoblocking: (1) the need to be 'anywhere but' a particular country, which would be the concern of free speech activists and (2) to appear to be in a specific place, in order to watch a TV show available only in that location. Geoblocking and VPN should be regarded as neutral tools and the law should be qualified so that people don't have to worry about negative legal implications of using them.

Although, as Trimble observed, geoblocking has been vilified, panelists noted some positive aspects. For example, Hall has blocked Chinese IP addresses from his josephhall.org website because users and search engines from the country were using up so much bandwidth. Mike Godwin noted that geoblocking could be used as a form of protest, such as when some sites blocked requests from the USA during the SOPA/PIPA 'going dark' protest. Trimble suggested that there are situations and places where geoblocking has legitimate purposes and can be likened to someone placing a lock on their own house when they leave. The same lock on a polling station at election time would be problematic. It is a tool that can be misused like any other technical tool. Smith suggested that issues arise when geoblocking is over-incentivised or compelled.

> ***We are now seeing both of the two worlds envisaged by Johnson and Post: lowest common denominator of content enforcement and Balkanization based on terrestrial jurisdictions.***

Geoblocking or targeting?

Drummond stressed that geoblocking is often implemented reluctantly, as a less damaging alternative to global removal of content. He questioned why a targeting regime, in which users default to content on local domains but can still see content elsewhere if they take steps to do so, is not sufficient. This preserves the users' right to travel in cyberspace while for the most part ensuring that people see only local content, since the defaults are very powerful. This sort of regime handles the territorial problem quite well. Since people can get around geoblocking you are not getting a lot more law enforcement that way.

The right to travel in cyberspace

The idea of the right to travel in cyberspace provoked discussion. Trimble referred to her 2012 paper in which she had explored right to travel arguments. In the physical world there are limitations, such as needing a passport to travel abroad. In cyberspace, it is up for debate what kinds of limitations are appropriate in which situations. Drummond said that Google had always resisted geoblocking because while it did not deprive the whole world from seeing content in places where it is legal, it does eliminate the right to travel.

Smith observed that if your starting point is that your citizens, whether they were inside or outside your borders, should under no circumstances be able to access content governed by a different legal regime, then you are unlikely to think that a targeting regime works well. However, this approach imposes more restrictive borders than in the offline world. It is something more like the Berlin Wall, whose purpose was to keep people in. In cyberspace, keeping information out keeps people in.

Granularity

Some discussion centered around granularity. Hall argued against establishing default rules that would effectively require constant, granular tracking of Internet and mobile users' location, undermining their privacy. Godwin commented that we do not know what 100% effective blocking of objectionable content looks like except to totally Balkanize the Internet. We are now seeing both of the two worlds envisaged by Johnson/Post: lowest common denominator of content enforcement and Balkanization based on terrestrial jurisdictions.

Trimble commented that a digital passport would need, at a certain level of abstraction, information about where the user is from and what kind of content is available to it.

> ***Jurisdiction rules that effectively require constant, granular tracking of Internet and mobile users' location can also undermine their privacy.***

A prohibition arms race?

A recurring theme in the discussion was the tendency towards a prohibition arms race: blocking followed by circumvention followed by action against circumvention. At each stage prohibitions tend to become more general, leading to increasing negative effects as legitimate behaviour is affected. Hall noted that the use of VPN tunnels can be countered by a service blocking VPN exit points, which prevents those who need to use VPN from using the service. However, one new tool—called Streisand—runs multiple flavors of VPN, allowing increasing agility to users seeking to circumvent censorship. For example, the Streisand tool can make all communications look like credit card transactions, which censors are loathe to block, lest they impact Internet e-commerce in their region. As Hall and others have seen emerging in the field, governments may now be deploying machine learning techniques—effectively artificially-intelligent systems that can "learn" to spot leaks in the Great Firewall—to counter these new tools.

Trimble asked whether circumvention of geoblocking is a widespread practice leading to significant erosion of territoriality or had negligible spillover. Should we abandon attempts to achieve territoriality, or regulate the spillover?

Smith commented that Johnson/Post had predicted that attempts to preserve borders in cyberspace would prove futile. However, we have to bear in mind what timespan we are

considering. We don't know if we are witnessing the brink of a new era of a Balkanized Internet or the last thrashings of the dinosaurs.

Big company rules for small actors?

The discussion moved on to the effect on small actors of making laws on the basis of what the large players can do, such as geoblocking. Will the local online newspaper simply block the rest of the world to avoid the problem of understanding the laws of every other country? What other unintended consequences may arise from geoblocking becoming a norm, if indeed it is a norm?

Godwin observed that Google has the resources to be responsive and make discriminations among cases. The chances are a new market entrant would not be able to do that. This raises the barrier to entry. Trimble emphasized the importance of the possibility of choice. A small newspaper told that it could not geoblock might have no option but to obtain a global or regional copyright license, which it might not be able to afford.

It was suggested that countries might adopt a twin strategy of controlling large companies providing protocols such as VPN through licensing requirements, and putting small disruptive technologists out of business. Hall said it would be unfortunate if pressure put on such developers led to them having to remain anonymous in order to develop secure communications tools.

The possibility of crafting different laws based on different sizes of company was also raised. That would require consideration of what is meant by size, when a small company is capable of having a large effect on the Internet.

Intellectual Property

Summary by Annemarie Bridy
Watch Video

Panelists:

- Annemarie Bridy - Professor of Law, University of Idaho; Affiliate Scholar, Stanford Center for Internet and Society
- Ben Sheffner - Senior Vice President & Associate General Counsel, Copyright & Legal Affairs, Motion Picture Association of America, Inc. (MPAA)
- Corynne McSherry - Legal Director, Electronic Frontier Foundation
- Alex Feerst - Head of Legal, Medium

From the Agenda:

> *Is intellectual property uniquely eligible for global enforcement, because it is relatively harmonized around the world by treaties? Are territorial restrictions so baked into copyright licensing and business practices that the law must compel geoblocking on copyright grounds? When and why should the law push in the opposite direction by prohibiting geoblocking—as the EU recently announced it would do for some copyrighted content?*

****

The topic of this panel was cross-border issues in the online enforcement of intellectual property rights. The speakers brought a range of perspectives from the movie industry (Ben Sheffner), the public interest sector (Corynne McSherry), academia (Annemarie Bridy), and the tech industry (Alex Feerst).

The panel began with a discussion of *Equustek Solutions Inc. v. Jack*, a case then pending before the Supreme Court of Canada.[1] In the case, Google challenged a lower court's injunction requiring it to remove search results not only from its Canadian services, but globally. The sites belonged to the defendants, who were accused of trade secret misappropriation and trademark infringement. The defendants fled Canada during the course of the litigation, which led the court to strike their defenses as a sanction. The trial court ultimately issued an order enjoining the

[1] 2015 BCCA 265, *available at http://www.courts.gov.bc.ca/jdb-txt/CA/15/02/2015BCCA0265.htm*. The panel discussion predated the Canadian Supreme Court's subsequent decision, which affirmed the appellate ruling.

defendants from using *Equustek*'s trade secrets and from selling infringing inventory. The defendants predictably disregarded the court's order. They continued to sell products from various websites they controlled from indeterminate locations. *Equustek* asked Google to globally remove search results for the defendants' websites, which Google refused to do. Google agreed only to remove infringing URLs from results on its Canadian search service at www.google.ca. *Equustek* argued before the trial court that Google should be compelled to do more.

The trial court agreed. Specifically, the court held that (1) the plaintiffs were suffering irreparable harm by the defendants' ongoing sales of infringing inventory on the Internet; (2) Google was inadvertently facilitating that harm through its search engines; (3) the plaintiffs had no alternative to the application brought against Google; (4) the relief sought against Google would not cause Google any expense or inconvenience, and was only a slight expansion of what Google agreed to do voluntarily; and (5) for the orders against the defendants to be effective, even within Canada, Google must stop displaying the defendants' websites on Google's search results on all of Google's websites, not just www.google.ca.

Google appealed the trial court's decision and asked the Court of Appeals to set aside the order. Google made three ultimately unsuccessful arguments. First, Google argued that the order was contrary to both Canadian jurisprudence on orders that restrict freedom of expression and parliamentary guidance on the grant of injunctions against search engines. Second, Google argued that the trial court erred in applying rules concerning injunctions against non-parties to the litigation before them. Finally, Google argued that the order violated principles of international comity. The Court of Appeals rejected all of Google's arguments and upheld the worldwide injunction. In a ruling that post-dated the panel discussion, the Canadian Supreme Court affirmed.

Equustek is a controversial case because the court's order required Google to de-list search results worldwide—not just from the company's Canada-targeted service at www.google.ca, which the company said was used by some 95% of its customers in Canada. In effect, a Canadian court asserted its authority over the contents of search results globally, for Canadians and everyone else. The extraterritorial reach of the Canadian court's order raised difficult questions about the relationship between law and borders in cyberspace.

After summarizing the case, Sheffner discussed the MPAA's position concerning the issuance of non-party injunctions against Internet intermediaries in cases of online infringement where defendants disregard court orders entered against them and thereby frustrate plaintiffs' ability to realize their remedies. He described a four-factor test proposed in an amicus brief filed in the Supreme Court of Canada in *Equustek* by the Fédération Internationale des Associations de Producteurs de Films (FIAPF), a trade group of which the MPAA is a member. Under the FIAPF's proposed test, the four factors a court should consider are: (1) the likely effectiveness of the order in remedying the harm caused to the claimants, and the availability of alternative remedies; (2) the cost to the intermediary of implementing the order; (3) the impact of the order on freedom of expression; and (4) evidence that the order will have extraterritorial effect in a manner that offends comity. Under this test, Sheffner asserted, the order issued in *Equustek* was

proper and should be upheld. At the same time, he suggested, the test would not support global removal based on speech-restrictive laws that vary widely between countries, such as laws against blasphemy.

McSherry argued that such an approach would not adequately protect speech and due process rights around the world, and said that a ruling in *Equustek*'s favor would set dangerous precedent. She described two alternative multi-factor tests presented to the Canadian Supreme Court in amicus briefs filed by the EFF and human rights organizations. EFF recommended that the Court consider six factors before issuing an order against a non-party online intermediary: (1) whether the order would offend another (relevant) State's core values; (2) whether the plaintiff made a strong prima facie case on the underlying claim; (3) whether the defendant is causing substantial irreparable harm; (4) whether the order is narrowly tailored to address that harm; (5) whether the order is technically feasible and effective; and (6) whether the balance of equities favors issuance. Human Rights Watch and other human rights organizations in a joint brief suggested to the Court a test derived from the International Covenant on Civil and Political Rights. Under that test, the Court would consider (1) whether the order is valid under domestic law; (2) whether it is necessary to protect rights, national security, public order, public health, or morals; and (3) whether it is proportional in light of impacts on freedom of expression and alternative means of achieving the goal. Applying these tests, both EFF and the human rights organizations urged the Canadian Supreme Court to overturn the lower court's decision.

Amicus briefs from trade groups and civil society organizations in* Equustek *proposed competing legal tests for cross-border orders to restrict online information.

Sheffner and McSherry agreed in principle that protecting freedom of expression is important in these kinds of cases, and that consideration of conflicting speech norms between relevant States is necessary, both in its own right and as an element of the international comity analysis. McSherry expressed concern that the ability of national courts to issue Internet-wide injunctions against online intermediaries could lead to a "race to the bottom" in which plaintiffs forum shop for courts in jurisdictions with weak speech norms and strong copyright laws. She emphasized that applying principles of comity to cases involving conflicts over online content removal requires consideration of whether the relevant jurisdictions recognize fair use and, if so, whether they recognize it to the same extent. In response to concerns about asymmetrical fair use norms between jurisdictions, Sheffner asserted that the MPAA does not seek injunctions against online intermediaries in "close" copyright cases, meaning those in which fair use would be a colorable defense in the jurisdictions that recognize it. He expressed a belief that comity concerns are not triggered by the injunctions the MPAA seeks because the MPAA targets only "blatantly infringing sites" that have no legitimate claim to fair use.

Bridy, the panel's third speaker, shifted the discussion of global content blocking from the courts to the Internet's technical infrastructure. What if, she asked, the jurisdiction of courts over

nonparty intermediaries could be made irrelevant to anti-piracy enforcement? What if right holders could get the keepers of the global Domain Name System (DNS) to start policing content on websites and unilaterally suspending or cancelling domain names in response to their complaints?

Responding to these questions, Bridy described recent efforts by right holders to avoid the "law and borders" issues raised in cases like *Equustek* by implementing, with ICANN's cooperation, a privately ordered framework for notice and blocking within the DNS. The framework is outlined in a "trusted notifier" agreement between the MPAA and two registry operators—Donuts and Radix—that control hundreds of new global Top Level Domains (gTLDs), including .movie, .wine, and .computer.

The backstory on the MPAA-Donuts/Radix agreement begins with ICANN's launch in 2011 of a substantial expansion of the Internet's domain name space through the introduction of over a thousand new gTLDs. Right holders saw in the new gTLD process an opportunity to inject anti-piracy obligations into the hierarchy of private agreements governing the relationship between ICANN and the various downstream entities that administer the DNS. The MPAA and the Recording Industry Association of America (RIAA) successfully lobbied within ICANN's multi-stakeholder governance forum for a "flow down" provision in the 2013 ICANN-Registry agreement. The provision requires registries to include in their contracts with registrars a provision that requires registrars to include in their contracts with registrants a provision that prohibits copyright infringement and promises consequences for infringement, including suspension of the domain name.

Citing the prohibition on copyright infringement in the ICANN contracts as their legal justification, Donuts and Radix have agreed to act as private investigators and adjudicators of the MPAA's complaints that domain name registrants are operating "pirate sites." Under the agreement, the registry operators treat MPAA's complaints "expeditiously and with a presumption of credibility." The standard for the submission of a complaint is "clear and pervasive copyright infringement." Before approaching the registry, MPAA must go first to the registrar of record and the site's hosting provider. However, if it is not satisfied with the outcome of those interactions, the registry operator becomes the private court of last resort.

Bridy identified a host of normative concerns relating to the trusted notifier framework:

- There is a presumption of guilt for accused registrants.
- Complaints target (and sanctions affect) an entire second-level domain rather than specific content.
- There is a lack of clarity about what constitutes "clear and pervasive copyright infringement."
- There are no established procedures for registrants to contest complaints and/or appeal sanctions.
- There is a lack of transparency about sanctions taken under the agreement and no mechanism for public reporting.

The final panelist, Feerst, offered a practical perspective on "holes" in the DMCA. One jurisdiction-related issue arises when right holders outside the US send DMCA notices to US-based platforms. Do such notices effectively signal acceptance of US legal jurisdiction over the dispute, and potentially even waiver of remedies under other countries' laws? Must right holders assert only copyright claims that are valid under US law, or can they use the DMCA to assert claims under the law of the sender's country? Has notice and takedown for copyright become de facto harmonized through platforms' global application of the DMCA?

> ***Has notice and takedown for copyright become de facto harmonized through platforms' global application of the DMCA?***

Another issue arises from publishing platforms' increasing reliance on enterprise cloud services. Feerst explained that many user-generated content (UGC) platforms, including Medium, do not operate their own servers, but instead rely on third party hosting providers like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform. The cloud provider hosts the platform's content, including UGC. This arrangement creates ambiguity and complexity under the DMCA—as Feerst illustrated with the example of a DMCA takedown notice Medium received, via AWS, from the government of Ecuador for images published by a user on Medium.

First, the arrangement creates multiple entities that could be viewed as online storage providers—a content platform as well as its upstream cloud provider. Right holders who want to file DMCA notices that target content appearing on a content platform like Medium might logically be expected to file those notices with the platform's designated DMCA agent. Instead, however, they might file notices directly with the upstream cloud provider. This creates serious questions under the DMCA: are both the platform and the cloud provider "hosts" with removal obligations? What is the permissible turnaround time for "expeditious" removal in this two-host situation? Can the platform host send a counternotice to the cloud provider? The problem is exacerbated by the cloud host's limited technical options: it may be able to shut down a platform's entire website and service, but not able to remove an individual item of UGC from that platform. Finally, the chain of contractual relations running between the intermediaries may, in practice, displace the law. The content platform may be asked to remove the content in question with a deadline imposed by private contract, with a time limit that may be less flexible than the DMCA's standard of "expeditious" removal. If the content platform fails to remove the disputed content, it risks breach of its contract and potentially existential consequences for that breach (at the extreme, termination of the contract and, as a result, removal of all hosted content). Whereas a content platform would risk a lawsuit from an aggrieved right holder if it chose to ignore a DMCA notice directed to its own DMCA agent, it potentially risks its entire business operations if it chooses to ignore a DMCA notice directed to its cloud provider. The DMCA risk calculus for smaller platforms that outsource hosting to major cloud providers is thus very different than it is for larger platforms that operate their own storage facilities.

In a world where web-based publishing platforms routinely rely on cloud storage vendors to host their UGC, an individual platform can find itself between a rock and a hard place when it comes to copyright takedown demands. As the apparent-but-not-actual host of its users' content and as a user itself of the cloud services that actually store the content, a platform is potentially liable on two fronts if it resists takedown demands: to right holders for infringement and to its storage provider for breach of contract/Terms of Service.

In further discussion, the panel considered the jurisdictional significance of the two-host situation. A platform's relationship with the cloud provider may also effectively put it within reach of claimants around the world—including in countries where the platform itself is not subject to jurisdiction. Even if both the user who creates content and the platform to which he posts it operate entirely within one country, the same is likely not true of the cloud hosting provider. Its international business operations may create the basis of jurisdiction for claims affecting content on small and medium-sized platforms around the world. The consolidation of Internet infrastructure in the hands of a few major hosting providers may thus create a new, and under-considered, legal and practical mechanism for cross-border content removal.

Data Protection and the Right to Be Forgotten

Summary by Joris van Hoboken
Watch Video

Panelists:

- Bruce Brown - Executive Director, Reporters Committee for Freedom of the Press
- Mathias Moulin - Deputy Director, Commission Nationale de L'Informatique et des Libertés
- Luiz Moncau - Intermediary Liability Fellow, Stanford Center for Internet and Society
- Joris van Hoboken - Senior Researcher, University of Amsterdam

From the Agenda:

> *One of the biggest Internet jurisdiction disputes of our time is Google's disagreement with European Data Protection regulators over global removals of search results based on EU "Right to Be Forgotten" law. What will happen there, and what should happen? If courts in the EU or elsewhere find jurisdiction based on the unique territoriality and processing provisions of Data Protection law, what precedent does that set? How will it shape cross-border enforcement orders in "libel tourism" cases, copyright cases, or other claims outside the Data Protection framework?*

****

This panel addressed the right to be forgotten (RTBF) from a global perspective, presenting points of view from relevant stakeholders and academic researchers from different regions. As established in the Court of Justice of the European Union's 2014 *Google Spain* case, this is a right under data protection law for individuals to request that search engines de-list specified results appearing in response to a search for the individual's name.[2] While search engines may decline to de-list results based on public interest considerations, the RTBF is still far broader than de-listing or removal rights in many countries, including the United States. This is especially the case since de-listing can also be requested for information that lawfully published online.

[2] *Google Spain SL v. Agencia Española de Protección de Datos* (AEPD), Case C-131/12, May 13, 2014

After a round of opening statements from the panelists, summarized below, a lively, and at times provocative, discussion with the audience took place about the conceptual boundaries of the RTBF, the legitimacy of extra-jurisdictional impacts on free speech, and the possibility of resistance in view of the RTBF's impact on the free flow of information online and the right to freedom of expression of Internet users and publishers. The discussion clarified the potential of the RTBF to continue to cause principled conflicts over the extent to which national laws should be allowed to impact the free flow of information outside of national borders, and the difficulties of reconciling fundamental differences in value systems in practice if jurisdictional overlapping claims become more common.

Bruce Brown's presentation opened up the question of stakeholder participation in the RTBF debate, specifically about the role of news organizations and organizations defending a free press in the debate about the legitimacy of a RTBF and its proper application. Brown clarified that press organizations until now had not taken a very leading role in the debate. In the debate about the RTBF, the news industry and press organizations cannot be seen as monolithic. At the moment, it appeared to him that they were more in an amicus role rather than in the driver seat when it comes to free speech norm creation on the Internet. Related to this, Brown also raised the question of which free speech rights to focus on in the RTBF debate. Should the focus be placed on the rights of Internet users and readers? Or should the emphasis be on the rights of speakers and publishers to reach an audience with their publications in different parts of the world, including through search engines? As the potential impact on the rights of speakers and publishers was put forward in this presentation, the presentation also raised the question of what news organizations know about the way in which the RTBF is impacting the dissemination of their materials to online readers. Would it be possible for news organizations to provide data on the impact of RTBF de-listings, as part of their readership analytics? Perhaps, news organizations could play a constructive role in the debate by offering statistics, complementing transparency reporting efforts in the online services industry.

> ***In the debate about the "Right to Be Forgotten," the news industry and press organizations cannot be seen as monolithic.***

Mathias Moulin presented the perspective of the French Data Protection Authority, the Commission Nationale de L'Informatique et des Libertés (CNIL), and defended the way in which the RTBF could be seen as the legitimate application of French data protection law. First, Moulin presented some figures (the absolute and relative number of requests, de-listings, removals for other reasons than the RTBF, and involvement of CNIL in enforcement of the RTBF), concluding that the effect of the RTBF in practice was rather limited. If anything, the discussion of these figures may have raised the question for the audience of how one would assess the importance of a particular website remaining accessible through a name search, and on what basis.

Second, Moulin clarified how the RTBF is the result of the application of long-standing principles of European data protection (national laws that have existed since the 1970s and were harmonized in the Data Protection Directive) and European fundamental rights law, in which freedom of expression has to be balanced with an equally important right to privacy. Moulin clarified that what may have been new about the RTBF, from the perspective of CNIL, was simply the result of regulators not having managed to apply existing laws to search engines before the RTBF ruling. (This argument is not convincing to the author of this summary, considering the conclusions reached by the Article 29 Working Party in 2008 on how to apply the Data Protection Directive to search engines).

Third, Moulin addressed the question of whether the RTBF should be considered a threat to freedom of expression. He answered this question in the negative, noting that the source of the content is not affected, and the de-listing only takes place for name queries. In addition, he pointed out that the RTBF can only be exercised by the affected individual in relation to his personal data and cannot affect historical events, and the application of the RTBF requires that the interests of Internet users in access to the information is properly taken into account, which should guarantee that if these interests should override the interests of the individual in de-listing, the request should not be granted.

Fourth, Moulin clarified the CNIL's point of view with respect to the extraterritorial effect of de-listings, specifically its view that de-listings, when granted, should be granted on all global and local versions of a search engine service. He asserted that the purpose of European law is not to dictate which information Internet users outside of Europe can and cannot find on the Internet, but simply to ensure that the fundamental right to data protection is respected by companies falling under European jurisdiction. Because everything the Google search engine does with data should be considered a single "processing" under the law, individuals' rights to prevent such processing cannot be limited to a single national version of the search service. Nor can a data subject's fundamental rights vary depending on who is looking at the information.

> ***As French privacy regulators see it, an individual's fundamental right to privacy cannot vary depending on who is looking at the information, or where the viewer is located.***

In the discussion with the other panelists and the audience that followed, Moulin was asked whether the question of extraterritorial application might involve a more nuanced assessment, including for instance consideration of whether the information would have a potential international readership, where the speaker and his main audience were located, etc. In response to this question, Moulin suggested that it may not be CNIL's primary aim to provide the most nuanced substantive interpretation of how to apply the RTBF. Instead, CNIL's chief aim would be to establish, in court, that it has the power to require a global de-listing, when relevant, in its dealings with an international Internet company such as Google. Thus, for CNIL, the legal settlement of its global jurisdictional reach as regards internationally operating data controllers

appears more important than the proper settlement of individual RTBF requests and balancing of privacy and freedom of expression, also in a global perspective. The RTBF context may simply present an attractive opportunity for CNIL to settle these matters under European law.

While this may come as no surprise to some, the respect for diverging regional norms, and the collateral damage for globally operating search engines and the free speech interests of Internet users, including in Europe, do seem to warrant a more careful approach to this question of extraterritorial reach. In addition, how workable is such an approach in practice? How can the principle of judicial restraint in cases of overlapping and competing jurisdictional claims re-inform the debate about the proper enforcement of data protection as regards search engines? It was clear during the panel, and remains clear today, that the last word has not yet been spoken about these issues.

As mentioned, the panel took a global perspective on the RTBF, representing the French perspective, discussed above, comparative perspectives from academic research, including from Luiz Moncau who also spoke about developments related to the RTBF in the Americas, specifically. Moncau furthered the point that a global discussion about the RTBF requires conceptual clarity and an understanding of the legal systems in which developments are emerging. Are RTBF claims data protection law related, or emerging in other areas of law? Is the RTBF a right with respect to the historical record? Is it a right to get certain information erased, or only to get information de-listed from search engines? From a legal perspective, what is put forward as the basis for a RTBF? A right to one's personal information online? A right to the protection of one's reputation and dignity as a person? Moncau discussed a number of RTBF related cases in the Americas, ranging from cases in Mexico and Peru that were similar to the cases in the EU targeting search engines on the basis of data protection law, to cases in Brazil, where no data protection exists and something like a RTBF exists in the context of republication of information about criminal convictions.

Moncau ended his presentation with his answer to the question of clashing jurisdictional approaches. Specifically, he argued that jurisdictional caution is warranted, as he does not see any growing acceptance of countries letting other countries restrict the free flow of information on the Internet in their territory. And indeed, a future in which a European global or extra-territorial application of their RTBF would affect access to information of Internet users in the United States clearly runs counter to commitments to freedom of expression in the US, including search companies operating from the US. Even if the CNIL were successful in convincing European courts that Google must de-list search results globally, instead of merely for localized versions in Europe, this could hardly be expected to settle the matter. One could even imagine those services affected seeking remedies in the United States to protect them against such jurisdictional overreach on the basis of the First Amendment.

Joris van Hoboken (responsible for preparing this report) discussed the RTBF from the perspective of different approaches to intermediary liability for online platforms. First, he clarified that the RTBF emerged in the void that was left by the Ecommerce Directive with respect to secondary liability for search engines, because the Directive establishes no specific safe harbor for information location tools. This void is important given the clear impact that

search engines, and searches for people's names in particular, can have on people's privacy and reputation. As European intermediary liability law did not provide for a clear answer to the liability of search engines for such harms, data protection and data protection regulators were able to step into this void and address this legal (right to effective remedy) and societal demand.

Second, van Hoboken clarified that categorical approaches to intermediary liability, such as the absolute immunity provided for in US law under CDA 230, are not sustainable under fundamental rights requirements in Europe. He, apparently provocatively for some in the audience, put forward the argument that CDA 230's absolute immunity would clearly violate the right to an effective remedy under the European Convention of Human Rights and the EU Charter. He also maintained that one typical argument—that certain types of obligations on intermediaries do not scale very well—does not carry the weight in European courts that some might want it to carry, as it runs counter to the general requirement that justice be done in individual cases, especially where the protection of fundamental rights is concerned. In view of these characteristics of the European legal environment, he recommended that relevant US-based services do much more to embrace the complexity (and diversity) of the European environment to arrive at a more sustainable model of intermediary liability for privacy and reputational harms.

Finally, van Hoboken raised some points with respect to the CNIL case about global de-listings. He argued that generally, in his view, CNIL does not have a very strong legal case, based on the CJEU ruling, the Data Protection Directive and the EU Charter of Fundamental Rights. A central argument for the global de-listing order is that otherwise, the de-listing is not effective. However, the question of what legal enforcement is appropriate should be answered in relation to the underlying goals of the enforcement, namely to prevent a disproportionate impact on the right to privacy through name searches. Thus, the goal of granting a RTBF request is not to prevent access to the material entirely. This implies that leaving certain channels open, including what could be considered extraterritorial channels, can be consistent with the EU RTBF itself, as long as those channels do not pose a disproportionate impact on the fundamental right to privacy.

Human Rights

Summary by Agustina Del Campo

Panelists:

- Agustina Del Campo - Director, Center for Studies on Freedom of Expression and Access to Information CELE at Universidad de Palermo
- Jason Pielemeier - Special Advisor and Section Lead, Internet Freedom, Business and Human Rights, Bureau of Democracy, Human Rights, and Labor, US Department of State
- Paul Schabas - Partner, Blake, Cassels & Graydon LLP, Toronto

From the Agenda:

> *Rights guaranteed under the Universal Declaration of Human Rights are supposed to be just that: universal. Human rights litigators have in some cases sought redress in one country's courts for harms in another; they are also often on the forefront in opposing national court orders that conflict with free expression and other fundamental rights. How does human rights law affect outcomes when different countries prioritize different rights—such as privacy or free expression? What unique issues are posed by human rights law for cross-border orders regulating online speech?*

****

Without a doubt, human rights law provides an important framework for the discussion of cross-border speech regulation. The International Covenant on Civil and Political Rights (ICCPR) in Article 19 clearly states the right to express opinions and ideas "regardless of frontiers" and the Internet is a particularly relevant tool and platform for the exercise of this right, both in its individual and social dimensions. There was a common underlying basic agreement among the different panelists as to the need to include a human rights perspective in content removal discussions, whether judicial, regulatory or legislative.

International human rights instruments expressly protect people's rights to express opinions and ideas "regardless of frontiers."

The three panelists shared the view that human rights law may and should contribute to determinations of cross-border speech regulation as well as content regulation and Internet regulation more broadly.

Paul Schabas presented first with a call for judicial attention to the principles of comity and proportionality. As an experienced media rights attorney and author to the amicus curiae brief submitted by the organizations Article 19 and Human Rights Watch, among other organizations, in the *Equustek* case—before the Supreme Court of Canada, he argued for the need to bring Article 19 of the ICCPR as a framework and structure to disputes involving or potentially implicating cross-border content removals.[3]

While comity was first understood as the need to respect and fulfill foreign judgments in other jurisdictions, after the libel tourism cases that put the US and Great Britain at odds in their interpretation of the right to freedom of expression *vis a vis* the right to reputation, a new understanding of comity arose. The new notion of comity, Schabas argued, is based on respect for different jurisdictions and their different understandings of the law. This new understanding in turn, brought judges, in Canada at least, to refer to judicial restraint in cases of cross border speech regulation. And this is precisely the basis for the argument in the *Equustek* amicus brief.

In *Equustek*, like in the French Data Protection Authority's global de-listing decision on the "Right to Be Forgotten," Schabas suggested that the Courts in Canada are overreaching their own jurisdiction, extending it beyond their borders. And like the *Google Spain* "Right to be Forgotten" case,[4] there is no mention of the principle of proportionality to frame the reasoning for the decision-making process. As Schabas, and Article 19 and Human Rights Watch argued, there is a need to look at content removal orders from the standpoint of international human rights law, particularly Article 19 of the ICCPR. And while Article 19 has exceptions, limited and narrowly tailored, it is for the States to interpret and balance them within a range of interpretation consistent with the ICCPR. Where one State interprets a universal right in a manner that is permissible within the "margin of appreciation," other States should respect that interpretation and not seek to impose their own, different understanding of the right. There is a recognition that we have common values that need to be balanced per the proportionality test, taking into account the impact on free expression, the impact on intermediaries, the efficacy of a decision, etc. And there is also a need to take comity into account, bearing in mind that if Canada

[3] Brief of Human Rights Watch, Article 19, Open Net (Korea), Software Freedom Law Centre and Center for Technology and Society, *Google v. Equustek*, *available at* https://cis-static.law.stanford.edu/cis/downloads/HRW Equustek.pdf.

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

adopts an overreaching decision and expects it to be complied with, other States, including those not respectful of human rights, may do the same and expect Canada to execute their decisions.

Next in order, Jason Pielemeier, speaking in his personal capacity, described three fact patterns that frame important challenges for policy makers.

The first fact pattern was that of the *Kidane v. Ethiopia* case, where a foreign government, using commercially available tools, is alleged to have illegally accessed the personal computers of a US citizen. The attack was allegedly triggered by Mr. Kidane's vocal and organized opposition to the hacking government, the government of Ethiopia. The case is being appealed after a District of Columbia district court decided the Wiretap Act doesn't create a right of action against a foreign State in US courts.[5]

The second fact pattern concerned a State-directed cyber-attack against a company physically located in the US in retaliation for an act of expression considered offensive. The facts coincided with the Sony Pictures Entertainment hack, which the US attributes to the government of North Korea.

The third fact pattern related to a sophisticated and novel form of Distributed Denial of Service (DDOS) attack against Github attributed by cybersecurity experts to the Chinese government in April of 2015. The fact pattern involved the planting of malicious code into email traffic to direct it to unwittingly attack websites which hosted content that would otherwise be censored by the attacking government.

Each fact pattern, as explained by Pielemeier, clearly restricts the free flow of information. However, calling them human rights violations, particularly under the ICCPR, would imply that the ICCPR applies extraterritorially (outside of areas under the responsible government's "territory and jurisdiction"), which runs against the official position of the United States and some other governments. The US government does not recognize the extraterritoriality of the ICCPR and interprets Article 2 narrowly. Article 2.1 states "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." The US government understands the ICCPR to apply only to people who are within its territory AND, rather than OR, under their jurisdiction. Some other governments and regional courts apply an "effective control" test to determine where jurisdiction may exist outside of a country's territory but it is unclear whether "effective control" could be established in any of the illustrative fact patterns.

If human rights law doesn't attach to the fact patterns described, then it is harder to conceptualize their relationship to existing norms and expectations, as well as to justify appropriate responses. The lack of an appropriate response could in turn create an incentive for the recurrence and multiplicity of such attacks. Pielemeier concluded by explaining that the US government is working with other governments to develop a broader set of norms for state conduct in

[5] The appeals court later affirmed this ruling. *Kidane. V. Ethiopia*, 851 F.3d 7 (2017).

cyberspace during peace time, and has on occasions called out these attacks as against existing norms but has stopped short of calling them human rights violations per se.

Finally, the third speaker Agustina Del Campo focused on the framework provided by the Inter-American system for the protection of human rights and what that framework may contribute towards the cross-border regulation of speech dilemma. The presentation started by describing the very strong protections that the American Convention and the Inter-American jurisprudence have set forth for the region. In the Inter-American system prior censorship is expressly prohibited and limitations may only be legitimate in the form of subsequent liability and following the three part test: legality, necessity and proportionality. Most of the cases heard by the Inter-American Court arise from violations caused by the judiciary in their interpretation of the balancing test, and pivot around proportionality issues. The Inter-American Court of Human Rights has set particularly strong standards to protect public interest expression, expression related to public officials or candidates, and speech related to human rights violations.

Having set the basic framework for the protection of freedom of expression, Del Campo described the framework for reparations developed by the Court in an effort to assess if and how they may affect content removal and cross-border speech regulation. International law dictates that a breach of international law carries a duty to repair it. The UN Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law propose four different means to repair human rights violations: restitution, compensation, satisfaction and measures of non-repetition.

The preferred means of reparation for the Inter-American Court is restitution. And it has ordered restitution in a number of freedom of expression cases, ordering both the production, the suppression and the restitution of information to its original format. The case of *Ivcher Bronstein vs. Peru*,[6] for example, concerned indirect restriction to freedom of expression—whereby Mr. Ivcher was deprived of his nationality in order to strip him of his rights and of shares he owned in a television network as retaliation for his editorial line. The Court ordered that the shares be returned to him. In *Herrera vs. Costa Rica*[7] and *Canese vs. Paraguay*,[8] two cases of disproportionate criminal defamation convictions, the Court found violations of freedom of expression and ordered the State to annul the convictions and exclude them from the defendants' criminal records. In *Herrera*, the Inter-American Court also reversed the domestic court's order requiring an online newspaper to link to that court's judgment. In most of its cases, whether on freedom of expression or not, the Court has also ordered that its decision be published in a government website for at least a year and at least once in a widely distributed national

[6] InterAmerican Court H.R., February 6, 2001, Series C No. 74, *available at* http://www.corteidh.or.cr/docs/casos/articulos/Seriec_74_esp.pdf.

[7] InterAmerican Court H.R., July 2, 2004, Series C No. 107, *available at* http://www.corteidh.or.cr/docs/casos/articulos/seriec_107_ing.pdf.

[8] InterAmerican Court H.R., August 31, 2004, Series C. No. 111, *available at* http://www.corteidh.or.cr/docs/casos/articulos/seriec_111_ing.pdf.

newspaper. And in the cases of *Manuel Cepeda Vargas*[9] and *Gomez Lund*,[10] the Court ordered that a documentary be produced to remember the victims and their particular contributions to their respective fields.

Per the jurisprudence cited to, in Del Campo's terms, there is broad protection of freedom of expression and a duty, once a violation is declared, to repair it effectively. Whenever possible, reparation should be through *restitutio in integrum*, which in some cases may entail the production and/or suppression of information. In this context, issues that may require further attention include: Under the strict test that the Inter-American system developed to protect free speech, what would a declaration of a violation to this right entail in terms of reparation? If upon a finding of a human rights violation, content is ordered to be produced, reinstated or removed, what should the scope for such an order be to comply with "restitution"?

Upon the panel finalizing their presentations there were a number of questions posed, starting with the conference hostess, Daphne Keller: A panel earlier mentioned a sort of arms race between geoblocking and circumvention and potential legal consequences for those utilizing and producing circumvention tools abroad. The US State Department Bureau of Democracy, Human Rights and Labor (DRL) has been financing the development and dissemination of tools that allow people to circumvent censorship. How is DRL dealing with the issues? And to the rest of the panel, are there human rights-based arguments to support the legality of the tools for circumvention? Particularly how does the "regardless of frontiers" language work?

Pielemeier confirmed that an important part of DRL's work includes supporting the development of circumvention tools to counter censorship. However, the case has not arisen where an organization that DRL was financing was found liable for that circumvention work. Still, he did agree with prior panelists that it's an important issue that could need to be addressed in the near future.

Going to the nature of geoblocking, Schabas manifested his concern as to the limitations that geoblocking poses to information seekers and the lack of effectiveness of such tools. He went on to describe, without naming, the case of a famous couple, where one was English and the other Canadian, who litigated in England seeking to geoblock certain content pertaining to them and eventually sought to implement such geoblocking in Canada as well. Per the example, he concluded, it would be very hard for different countries to agree on how to balance rights and there should be room to respect each other's decisions.

Professor Lea Shaver contributed an interesting question: we keep talking about comity, reciprocity and judicial restraint. However, the fact that we respect other's decisions doesn't necessarily mean that they will respect ours and vice-versa, or in the same kinds of cases. So, she asked, is it a zero-sum game, where it's all or nothing? Should there be rules on when

[9] InterAmerican Court H.R., May 26, 2010, Series C No. 213, *available at* http://www.corteidh.or.cr/docs/casos/articulos/seriec_213_ing.pdf.

[10] InterAmerican Court H.R., November 24, 2010, Series C No. 219, *available at* http://www.corteidh.or.cr/docs/casos/articulos/seriec_219_ing.pdf.

extraterritorial jurisdiction should be acceptable and when it shouldn't? What lines could be drawn for when content should be removed cross-borders or not?

Among the panelists, some considered that human rights norms were not that clear and human rights conventions have built in flexibility that challenge their universal application for these disputes. The lack of a universal court that could eventually resolve these issues came up as an issue that adds to the argument. However, others considered that the interpretations and guidelines of the different human rights supervisory bodies are not that different and may provide an underlying basis for the discussion. The issue remains, though, as to how to deal with States that are not a party to any human rights treaty?

> ***Might human-rights-respecting States agree not to apply their laws extraterritorially, when the remedy granted in one State would violate human rights as understood by the other?***

Ambassador Eileen Donahoe then asked: Among those that have agreed with the ICCPR, could human rights law provide a minimal bottom line? Can/should a regime be created for rights-respectful States, whereby per some basic rules, no extraterritorial application will be allowed if the remedy sought implies a violation of a human right per the understanding of another?

Pielemeier addressed the question and noted that one possible basis for determining when national law should apply extraterritorially could be the distinction in human rights law between "gross" and ordinary violations. He warned that certain decisions and standards, regardless of the jurisdictional reach, posed issues and concerns, like the "Right to Be Forgotten" decisions. These kinds of decisions generate dangerous precedents for countries looking for excuses to censor speech. Still, some norms can be developed among rights-respecting States and there are efforts underway already, like those being produced through the Freedom Online Coalition, that are moving in that direction. With that, the panel ended.

Mutual Legal Assistance and Law Enforcement Access to User Data

Summary by Albert Gidari
Watch Video

Panelists:

- Albert Gidari - Director of Privacy, Stanford Center for Internet and Society
- Jennifer Granick - Director of Civil Liberties, Stanford Center for Internet and Society
- Nathaniel Jones - Assistant General Counsel, Microsoft
- Andrew Woods - Assistant Professor, University of Kentucky College of Law

From the Agenda:

> *Lawyers and activists concerned with law enforcement, surveillance and privacy have long debated the rules that should govern cross-border requests for Internet platforms to disclose user data to law enforcement. The Microsoft Ireland case and mutual legal assistance treaty (MLAT) and Electronic Communications Privacy Act (ECPA) reform discussions in the US have added new urgency to this issue. Do lessons and insights from that discussion help us to think through the cross-border content regulation issues raised in this conference? How should the debate over cross-border data requests be informed by a broader understanding of the problems of international content regulation?*

****

The Law, Borders, and Speech conference at Stanford's Center for Internet and Society asked the important question: Which countries' laws and values will govern Internet users' online behavior, including their free expression rights? The conference used the landmark article written in 1996 by David G. Post and David R. Johnson to examine whether twenty years on their conclusions still held true. Post and Johnson had concluded that "[t]he rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply." They proposed that national law must be reconciled with self-regulatory processes emerging from the network itself.

The conference panels addressed how we reconcile differences in national laws governing speech today, and asked how we should be reconciling them; what are the responsibilities of Internet speakers and platforms when faced with diverging rules about what online content is legal; and whether users have relevant legal rights when their speech, or the information they are seeking, is legal in their own country. For those interested in content regulation and intermediary liability issues, these topics are well-traveled and often discussed, but the conference added a panel on law enforcement access to user data—a topic that raises many of the same jurisdictional and prudential concerns as the assertion of power to remove or regulate content globally but which is seldom discussed in the same breath or in the same room as content regulation.

The goal of the panel was to look at the current practices and procedures of sovereigns demanding access to user data, and how providers respond to such legal demands, to glean any lessons applicable to the content regulation world.

The discussion opened with the observation that there is a century or more of established practices and procedure that is territorially-based for cross border evidence gathering. Our existing treaties and conventions all recognize the doctrine of territoriality when it comes to evidence gathering. That is, one country doesn't seize evidence from within the borders of another country without the searched country's permission and cooperation. From that simple principle arose mutual legal assistance treaties and international procedures for procuring evidence abroad that stood the test of time—until the Internet broke them.

No doubt, the rise of the Internet, Internet platforms, social networks and cloud computing has created significant problems for law enforcement (LE). It is obvious, really—the victim of a crime of fraud may be local, but the perpetrator is likely in one or more countries using one or more access providers to get online and one or more applications to commit the fraud. The evidence of the crime and the perpetrators are likely outside the victim's place of residence, presumably the locus of the crime. This is not unlike the most difficult content regulation problems where the content may be hosted in one country, where it is legally displayed by a publisher located in a second country where it is legal to speak the content, but the party harmed by the content is located in a third country where there is no practical remedy under that nation's laws.

There are international processes in place for LE to obtain evidence of the crime or to identify the perpetrators, but it is acknowledged that these avenues are at best cumbersome, slow, bureaucratic and inefficient. Going directly to providers in other countries does not work—most of the providers of interest have historically been in the US, but increasingly that is not the only case. The US, like most countries, has blocking statutes that prohibit disclosure of content other than to domestic government authorities. And post-Snowden, even if there was previously room for voluntary cooperation, that door has closed. This gives rise to frustration for the investigatory agencies as the evidence often is necessary or fundamental to prosecution.

But just as with content regulation, LE is not sitting on its hands waiting for international law to develop to solve the problem. Instead, we see the extraterritorial assertion of power to compel disclosures by providers located abroad. Law enforcement agencies, sometimes assisted by local courts, assert power and demand cooperation from providers—including by asserting that a

global platform is using facilities within the country by merely having a service that is accessible and therefore actually "within the jurisdiction," arresting employees who are present in the jurisdiction, and even blocking access to service to force cooperation.

In short, these agencies act extraterritorially. This is not a problem just for requests coming from outside the US, affecting only US providers. US law can also be the source of extraterritorial demands in other countries. Amendments to Rule 41 of the Rules of Criminal Procedure would permit a warrant to issue from any US court to remotely access a computer where its location is unknown. The same issue exists under the Cybercrime Convention. Article 32b of the Convention is an exception to the principle of territoriality and permits unilateral transborder access without the need for mutual assistance under limited circumstances. Rule 32b permits LE to access or receive, through a computer system in its territory, stored computer data located in the territory of another Party, if LE obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to LE through that computer system.

Some countries have also acted locally. They require data localization to facilitate lawful access to user information. Russia has been very aggressive of late in requiring local storage of data by online providers, but even local storage solutions are not ideal or fully effective—not all users whose data might be subject to local storage reside within the country for example. What choice or notice will those users have when corresponding or interacting with a user where localization applies?

> ***Providers cannot be in the position of deciding daily which nation's laws are going to be broken in responding or not responding to legal demands.***

The current system of mutual legal assistance treaties is inadequate to the task and in need of reform. Providers cannot be in the position of deciding daily which nation's laws are going to be broken in responding or not responding to legal demands. Not all providers can rely on the kind of argument raised by Microsoft in its ongoing case against DOJ—that data stored in Ireland can't be compelled for production on US process served on a US provider where the process lacks extraterritorial application.[11]

But legal victories based on territorial limitations of the sovereign's power may in the long run be a "log on the fire" of data localization. Governments will not be deprived of the evidence necessary to investigate and prosecute crimes, and the lack of an effective system to balance the needs of users, platforms and government agencies may yield worse precedents.

It is interesting to think about technology as a solution to the "problem"—such as the use of encryption for stored content. But governments see such "solutions" as obstruction of justice,

[11] *Microsoft Ireland: In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation* 829 F.3d 197 (2d Cir. 2016), *reh'g en banc denied*, No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017).

just as they see claims of jurisdictional protection by providers as avoidance of responsibility. Government mandates in the end can affect the lawfulness of the technology just as they can affect the disclosure of the data. As one panelist noted, "jurisdiction is a hack" to solid encryption, but that doesn't mean that technology should be ignored as a solution.

Just as with content regulation, interoperability among differing legal systems, and not harmonization, may be the more desirable goal. But at what cost to which principles? Probable cause and free speech in the US are values not shared globally, nor are they values that always trump other valid concerns of other sovereign interests.

> ***National law affirmatively obliges Internet companies to protect users' privacy against foreign law enforcement demands in some cases. By contrast, a company facing a foreign content removal demand almost never has legal obligations to protect users' speech rights.***

Over the course of presentations and conversation, panelists identified a number of points that may distinguish cross-border LE requests for user data from cross-border content removal demands.

- Legal obligations: National law affirmatively obliges Internet companies to protect users' privacy including against foreign LE requests in some cases, potentially creating a conflict with the law of the country whose LE is seeking the data. Under MLAT agreements, this situation may arise where the act under investigation is a crime in the LE's country, but not in the company's. By contrast, a company facing a foreign content removal demand almost never has legal obligations to protect speech rights of users, and thus is free to comply with the request even in cases where the speech is protected under the company's national law.

- Sources of law: LE requests for user data are governed by long-established—if increasingly archaic—laws and treaties governing data disclosure, and establishing territoriality as a governing principle. No comparable history or source of law exists for content removal.

- Available information: Companies may have to respond to LE requests without knowing for sure where the data sits, what the user's nationality is, or where the user may be physically located. Content removal requests rarely arise in such an informational vacuum.

- Technological differences: Tools like geoblocking may permit companies to comply with content removal demands on one nationally-targeted version of their service, while keeping the content available in other countries. Such territorially limited compliance does not have an analog in the LE context.

- Risk: While both LE data requests and content removal requests can affect Internet users' human rights, the worst case scenario for improper data disclosure—wrongful arrest and abuse of innocent people—may be considerably worse.

At the same time, the panelists identified a number of areas of similarity.

- Centralization exacerbates conflicts: As online information is increasingly processed by a relatively small number of intermediaries, these companies become chokepoints for information control and centralized repositories of data about user activity. These companies and the governments of their home countries will face increasing pressure to reach accommodations with governments around the world, both for content removal and user data disclosure.

- Lack of public information: The processes followed by companies in response to both kinds of requests are relatively opaque to the public, and may be unknown even to the affected user.

- Political consequences of non-compliance: Companies rejecting or disregarding foreign legal demands of both sorts risk offending government actors in those countries. The resulting political fall-out, such as data localization requirements, may harm both the Internet companies and their users.

- Courts are the wrong forum: Resolving these complex issues through litigation is unlikely to lead to sound policy solutions. Not all affected parties or interests will likely be heard, and parties must shape their arguments to existing, flawed law—rather than promoting more sensible balances that might be achieved through legislation or treaty negotiation.

Perhaps in the end there are more similarities between content regulation and cross-border evidence demands than practitioners in both areas might have imagined. The jurisdictional questions are largely the same; the pressures on platforms to be solution providers is enormous; and government frustration with provider push-back is the same in both worlds. It seems clear to those that deal with cross-border evidence collection that in the absence of an agreed upon international framework with safeguards to permit lawful access to data, more and more countries will take unilateral action and extend law enforcement powers to remote transborder searches either formally or informally with unclear safeguards. The same is true with content regulation.

Black Letter Law

Summary by Dan Jerker B. Svantesson

Panelists:

- Amy Keating - Senior Legal Director, Twitter
- Uta Kohl - Senior Lecturer, Aberystwyth School of Law, Aberystwyth University
- Lea Bishop Shaver - Professor of Law at Indiana University Robert H. McKinney School of Law; Visiting Professor of Law at UC Davis School of Law
- Dan Svantesson - Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University, Australia

From the Agenda:

> *Black letter jurisdiction law can seem poorly suited to the questions that face courts in cases about global content deletion. What legal doctrine should courts apply to grapple with concerns about a "lowest common denominator" Internet, subject to every country's speech prohibitions? Which institutions of national government should help shape these laws? Are laws from a company's home country—such as the DMCA for US companies, or Russia's anti-LGBT laws for Russian ones—uniquely able to compel global content deletion from those platforms?*

****

The topic of how well the tool of black letter law works in the Internet law setting is of course huge, and associated with obvious definitional challenges. To point to but one; how ought we define "black letter law" in our present legal culture where legal rules necessarily must take account of the technical reality in which they operate? Indeed, given Wikipedia's definition of "black letter laws" as laws that are "the well-established technical legal rules that are no longer subject to reasonable dispute," one may legitimately question whether we can speak of any real black letter law within our field of enquiry. Fortunately, however, the panel was asked to approach only the more concrete topic identified in the description above.

As the organizers no doubt had predicted, the angles adopted by the presenters were diverse, which sparked a fruitful and vibrant discussion, both amongst the panel members and with the broader audience. To truly do justice to the richness of the discussion would necessitate a transcript being produced.

Here, my humble aim is to bring attention to a selection of particularly interesting topics that were discussed. Thus, I am seeking to reflect the discussion rather than merely my own personal views on the topics discussed.

Even in our brave new technology-driven world, black letter law cannot be ignored

With the powerful regulatory influence of technology, we have been made to realize that black letter law certainly has its limits. There is no point in denying this, and useful models have been developed illustrating that law is just one part of a bigger regulatory picture. However, it is perhaps the case that, at least in the past, we have underestimated the power of black letter law, in that we have overestimated the impact of difficulties of enforcing judgments across borders. Our focus has been on the idea that States need the cooperation of foreign States to have their judgments enforced in those foreign States, and since the underlying structure for such cooperation generally is weak, lacking cross-border enforcement mechanisms undermines the role of black letter law.

The problem with this reasoning is that it focuses on foreign enforcement of extraterritorial claims, overlooking the power of domestic enforcement of extraterritorial claims. Courts and other bodies (such as Data Protection Authorities) are increasingly determined to impose their laws on Internet conduct, and the reality is that there are many different types of "market destroying measures" they can take domestically to achieve an impact extraterritorially. To see that this is so, one need only consider the number of instances where States have shut down, in their territories, entire platforms operated from abroad. Overall, this is a harmful trend characterized by excessive State responses. However, one can easily imagine less draconian "market destroying measures" being applied. Thus, applied appropriately, and in a measured, proportionate manner, the underlying jurisdictional idea of States exercising "market sovereignty" over the market they control is much preferable to the biggest threat to the Internet—inappropriate *global* blocking/deletion orders.

At any rate, one key point here—for our context—is that when speaking of law, as in black letter law, we need to acknowledge that law has teeth and can, most of the time, not be ignored.

Black letter law fails to provide sufficient certainty

While we can conclude that black letter law still matters, and is likely to continue to matter, we must also acknowledge that black letter law often fails to provide sufficient certainty; and this is particularly noticeable in the context of fast-moving information technology. If we also consider that the law often "outsources" decision-making powers to technology companies, the scale and scope of the problems associated with this uncertainty becomes clear.

For individuals, the problem is obviously manifested in that their rights may not be adequately protected. For the governments, this problem undermines their authority as well as their efficiency as regulators. Finally, for the technology companies, the problem is that they are placed in the unenviable position of being asked to interpret and apply unclear laws. And every decision they make in their interpretation and application of those unclear laws may

subsequently be scrutinized by courts or authorities and be held to be mistaken, subjecting them to penalties and bad press.

Law makers, including courts, must do more to achieve clear and predictable laws that at the same time are sufficiently flexible; a great challenge no doubt, but this must nevertheless be the aim.

Inappropriate global blocking/deletion orders

Where the laws of, let us say, France are only affecting what can be accessed online in France, there is a clear link between the State's coercive power and the effect of that power being exercised. One of the biggest challenges today is that too often courts and other bodies do not seek to play within such limits. There is a tendency to require *global* de-listing or blocking for just about every violation of local law. Of course, global blocking has a role to play for some types of content (such as child pornography materials), but not as a default position for every violation of local law.

Courts need to be much more careful. To address this, we need to pay much more attention to what we may refer to as "scope of jurisdiction". In addition to talking about personal jurisdiction and subject matter jurisdiction, we should discuss scope of jurisdiction, as in the question of what is the appropriate geographical scope of orders rendered by a court that has personal jurisdiction and subject matter jurisdiction?

Courts must realize that there is a correlation between the strength of their claim for personal jurisdiction and the legitimacy of the scope of jurisdiction, as in the geographical scope of the remedy they order. And in fact, for example in EU law we can already see scope of jurisdiction being clearly discussed as a matter of jurisdiction.

However, this may obviously also be characterized as a problem that falls within the area of remedies law. While jurisdiction and choice of law issues address these questions at the beginning of a lawsuit, remedies law approach them at the end of the litigation, when damages and injunctions are set.

> ***Jurisdiction and choice of law analysis addresses questions about online speech and borders at the beginning of a lawsuit. Remedies law can do so at the end, when damages and injunctions are set.***

It is a principle of remedies law that injunctive relief must be appropriately tailored, which can include geographic tailoring. After finding a violation and deciding that equitable relief is warranted, a court ought to explicitly consider whether its injunction should apply only to the particular party, to a single office, or more broadly. The choice of remedies thus offers another opportunity for lawyers to argue that a court's exercise of authority should be geographically

limited. In this context, it is important to explore the principles underlying the norm of limited injunctive relief, and how these might be applied to online activity that crosses national borders.

We ought to move past the substantive issues, and even the choice of remedies issue of whether an injunction will be appropriate, to think deeply about the range of possible forms that this injunction might take. Because at the end of the day, who wins matters, but what matters even more is what the court is going to do about it. How broadly will the court's order be designed? Prohibiting (or compelling) exactly what conduct? For how long? Where? These are questions of injunctive scope. Attorneys should be thinking about these questions from the very beginning of litigation. Some of these possibilities will be acceptable to your client. Others will not be acceptable. It can be a disaster if the judge drafts an injunction uninformed by your arguments as to what scope is appropriate. On the other hand, if you have in mind what you want that injunction to say (even if you lose) you can advance arguments from the very beginning to limit the damage. Thus, it seems reasonable to suggest that companies litigating online speech issues ought to think carefully about injunctive scope as part of their strategy. And arguments about diverging values on freedom of expression and privacy, and the technicalities of global takedown can help push courts to draft a more narrowly framed injunction when they feel they need to order some kind of restriction on speech.

Thus, this is clearly a problem where remedies experts and jurisdiction experts need to work together.

The impact of cultural differences

The important impact of cultural differences has already been hinted at in the above. More broadly, however, it can be argued that legal solutions are not necessarily the best ones (which admittedly undermines the role to be played by black letter law). This is exemplified in that, arguably, the most challenging conflicts today are not merely between tech companies and governments, or between different governments, but between user groups that are increasingly polarized; that content issues are increasingly not about what is legal, but about what is acceptable or civil. And as users are global, they have different views.

Perhaps we can prevent some of these problems from coming to court if there is greater humility and sensitivity to differing values. This debate still contains echoes of John Perry Barlow’s cyberanarchy sentiment that the Internet ought to be immune from regulation. This is perhaps rooted in a uniquely American sentiment of "sticks and stones may break my bones, but names will never hurt me."

It is troubling to some that so many Americans in this space take it as a point of pride to refuse to seriously entertain European sensibilities about (data) privacy and Holocaust denial. Or the social context for Indian blasphemy law also alluded to during the conference. Is this principled leadership in the defense of universal values, or a Silicon Valley parochialism? For companies who bear the social responsibility for Internet freedom worldwide, it is essential to be open to "foreign" views on the appropriate scope of freedom of expression, to seriously consider them, and to engage in a dialog with a spirit of humility and awareness of our own local perspectives.

> ***Many Americans take it as a point of pride to refuse to seriously entertain European sensibilities about privacy and Holocaust denial, or the social context for Indian blasphemy law. Is this principled leadership in the defense of universal values, or Silicon Valley parochialism?***

In this context, it should also be noted that, surrounding factors—such as how is the US seen, and how is the relevant technology company in question perceived—influence whether courts around the globe will seek to exercise jurisdiction over US technology companies. Thus, it is possible that a general stronger willingness to accommodate foreign views—going beyond mere legal compliance—will limit the risk of the relevant technology company being pursued by the, often limited, enforcement resources of foreign states. At the same time, US technology companies must obviously carefully evaluate whether the foreign cultural values in question are so far detached from the company's values so as to make it impossible to accommodate them. In the latter case, they may conclude that it is best to entirely avoid the relevant market.

Finally on this, in devising a litigation strategy, US technology companies must be mindful of the fact that, courts' desires to allow local plaintiffs to litigate locally is closely linked to conceptions of sovereignty. Thus, it may often be prudent to not only dispute jurisdiction, but to also tackle the underlying substantive legal issue. Indeed, in some cases, it may be strategically unwise to make what otherwise is a domestic dispute into a cross-border issue by disputing jurisdiction where the company in question has a substantial presence on the relevant market.

The 'presumption against extraterritoriality' in the online global order

It has been noted that territoriality and extraterritoriality are claims of authority, or of resistance to such claims that are made by particular actors with particular substantive interests to promote. Consequently, territoriality (or territoriality of law and order) is not a 'natural' state of affairs, but a legal construction created to protect certain interests. Furthermore, however ill-suited it may be for the global (online) market place (see further below), territoriality remains the norm or the default standard for legitimate authority. Under this thinking, anything extraterritorial is prima facie considered something 'outside the norm' and carries with it a strong whiff of illegitimacy.

The presumption against extraterritoriality is applied by the judiciary to interpret legislation and tells us that legislation applies to persons and matters within the territory of the state, but not to persons and matters outside the territory, unless the legislation evinces a contrary intention. Even though the presumption would appear to be highly pertinent in Internet cases—given that each State's regulation of online activity always has some extraterritorial effect—this principle has so far figured very rarely in Internet cases.

In the standard Internet jurisdiction case, judges simply find that the foreign online content or service provider has to comply with local law on the basis that a local injury is caused or a local

interest is affected by the foreign actor or activity. This means that the law and its application to the facts is either not treated as 'extraterritorial' at all (i.e., we are only regulating what occurs on our territory) or alternatively, the presumption is displaced, based on the thinking that the law's territorial overreach is justified as a legislative effort that simply seeks to redress a domestic injury caused by foreign conduct.

The most significant function of the presumption against extraterritoriality is that it advocates caution and restraint in extraterritorial regulatory assertions, saying that in the vast majority of cases it is inappropriate to extend the law and litigation to matters that lie outside the State's territory. Thus, the presumption is driven by the potential conflict of different laws and in recognition of each nation's sovereign authority and the desire for a harmonious global working order.

Looking at cases such as various US cases from 1996, to *LICRA v. Yahoo!* in France in 2001[12] and *Gutnick* in Australia in 2002,[13] to the recent *Equustek Solutions Inc. v. Jack* in Canada in 2014,[14] it would appear that the desire for a harmonious global working order has been rather limited amongst the courts to date. Typically too, the presumption against extraterritoriality is displaced in three different ways by Article 3 of the European Union's *General Data Protection Regulation* (entering into force in May 2018).

While on a technical legal level the result of this position signals the effective expiry of the relevance of the presumption against extraterritoriality, in broader regulatory terms the presumption reflects and embodies a global order based on state law. Where everybody regulates everything (or at least in principle asserts the right to do so) or where a system of regulatory allocation is entirely predicated of might over right (i.e. enforcement jurisdiction), its practical or principled utility and efficacy is under threat. Where France does not just regulate France but also the rest of the world and where this principle is extended to every other State, a State-based system of law and order has broken down and lost its *raison d'être*. From a more close-up, constructive perspective, the routine non-applicability or displacement of the presumption in transnational Internet cases requires its re-thinking and a re-framing. Such re-thinking would aim to reintroduce a measure of restraint and caution into competence assertions, so much so that not every foreign online provider who has contacts with local residents is always exposed to local law.

The problem of our focus on territoriality

Perhaps the biggest problem we have in black letter law is that our law on jurisdiction is grounded in the territoriality principle—the territoriality principle is the jurisprudential core of

[12] *UEJF & LICRA v. Yahoo!, Inc. & Yahoo! France*, T.G.I. Paris, May 22, 2000.

[13] *Gutnick v. Dow Jones & Co Inc.* [2002] HCA 56, *available at http://eresources.hcourt.gov.au/showCase/2002/HCA/56.*

[14] 2015 BCCA 265, *available at http://www.courts.gov.bc.ca/jdb-txt/CA/15/02/2015BCCA0265.htm*. The panel discussion predated the Canadian Supreme Court's subsequent decision, which affirmed the appellate ruling.

our thinking on jurisdiction. But it should not be. We all know that the territoriality thinking is a bad fit for cyberspace, but it is also increasingly obvious that the territoriality principle is a bad fit for the real world; just consider areas such as human rights law, environmental law, air law and so on. So the good news, if it can be seen to be news, is that we do not need to show that cyberspace is different; cyberspace is just one more illustration of the problems with the territoriality principle as such.

One proposed alternative jurisprudential framework for our thinking on jurisdiction is for us to focus on: substantial connection, legitimate interest and a balancing of interest. This has obvious parallels with what you find in the US Restatements, and for example in the comity thinking, in the doctrine of *forum non conveniens*, etc. Without exactly replicating any particular previous doctrine this proposal builds on established thinking and should therefore be easier to digest.

Some people will say that this is all fine but what we really need are practical solutions, not abstract theories. But what they then are missing is that where we apply a practical solution in a difficult case, we are often forced to interpret that practical solution in light of our underlying theoretical framework—in building terms, our theoretical framework is the foundation, and we all know what happens if we build on a flawed or weak foundation, we get into trouble and that is where we are now due to having built our jurisdictional thinking on the territoriality principle.

So only by starting with a new foundation for jurisdiction can we make sensible jurisdictional rules for the Internet.

Concluding remarks

All that remains for me to do here is to again thank the organizers of this terrific event, and to, 20 years belatedly, congratulate Professor Johnson and Professor Post on writing such an interesting article. There are few other articles that are equally deserving of sparking an event like this, and unfortunately, too many of the concerns to which they brought our attention remain unresolved today.

Real Power, Real Outcomes, Realpolitik

Summary by Daphne Keller
Watch Video

Panelists:

- Anupam Chander - Martin Luther King, Jr. Professor of Law, UC Davis
- Juniper Downs - Global Head of Policy, YouTube
- Min Jiang - Associate Professor of Communication, UNC Charlotte; Secretariat Member, Chinese Internet Research Conference
- Peter Stern - Policy Manager, Facebook
- Emma Llansó - Director, Free Expression Project, Center for Democracy & Technology

From the Agenda:

> *Sometimes, the most powerful forces shaping Internet content removal decisions don't come from the law. Companies' own discretionary Terms of Service or Community Guidelines often prohibit far more speech than the law does. How do these discretionary rules relate to national law—do they effectively displace it? Does public pressure from powerful countries, including their governments, shape content policies applied to speech around the world? The Council of Europe Human Rights Commissioner has said that States exercise authority - and must respect limitations grounded in human rights—when they pressure private Internet platforms to "voluntarily" remove content. Is this really a legal issue, or only a political one?*

****

This panel considered issues of national jurisdiction in relation to Internet platforms' voluntary content removal policies. These policies, typically set forth in Community Guidelines (CGs) or similar documents, prohibit content based on the platforms' own rules or values—regardless of whether the content violates any law.

Content removal based on CGs can raise important questions about the overall power of platforms to shape the information available to their users. Law Professor Anupam Chander captured this concern well in his panel contribution, which discussed Facebook's decisions to remove widely supported legal content, such as breastfeeding images. Chander's presentation was titled, aptly, "Should Mark Decide?" Removals based on CGs complicate the relationship between State and private power. Platforms typically set and enforce the same policies

worldwide, meaning that users from different cultural backgrounds—Stockholm versus rural India, for example—all operate under the same rules. This may flatten out regional differences in law and culture, displacing local values about speech, privacy, sexuality, and other significant topics.

At the same time, platforms' willingness to remove users' expression globally for violating CGs can be a source of global leverage for powerful States, as panelist Emma Llansó of the Center for Democracy and Technology pointed out. When governments convince a platform to ban or support content under CGs, they effectively achieve global enforcement of their own national norms, values, or laws.

In addition to Llansó and Chander, who provided framing observations, the panel included two company representatives, Facebook's Peter Stern and Google's Juniper Downs. Both discussed the platforms' internal practices and decision-making with respect to CGs. Communications Professor Min Jiang added a description of government practices constraining Internet content within China—practices which may be increasingly common in the rest of the world as more countries embrace a territorialized Internet.

The two company spokespeople, Downs and Stern, fleshed out internal thinking and processes used in enforcing CGs. Stern noted that Facebook's CGs are informed by law and human rights principles, but not grounded in the specific laws of any country. Rather, both he and Downs emphasized the companies' own founding missions as a source of direction and purpose for their policies. Both described extensive internal processes to set CGs standards, and discussed the difficulty of balancing conventional broad free expression protections with what Downs called the "freedom to belong." As both she and Stern noted, if CGs permit unfettered speech by all users, hostile or bullying voices may effectively prevent others from participating—which in itself reduces the array of viewpoints voiced on the platform. Downs also discussed the difference in policies for different Google products. For example, because completeness is important in the Web Search and Maps products, CG removals are more rare than in more community-oriented products like YouTube.

In an audience question, David G. Post pressed these speakers to consider alternatives to the internal standard-setting process. Expanding on a recurring theme of the conference, he asked about the potential for meaningful self-governance by the community of platform users. Might they, rather than companies or States, be consulted and relied on in establishing CGs? Both platform representatives talked about their existing efforts to listen to thought leaders and ordinary users, and to look to civil society groups as a proxy for user perspectives. As Stern pointed out, though, the diversity of users and preferences would make for a wide array of input—likely leaving companies to decide CGs at the end of the day in any case.

Chander, too, raised more pointed questions about internal processes, focusing on the enforcement of CGs. As an example, he identified Facebook's decision not to remove a post from then-candidate Donald Trump, which users had flagged as violating the company's hate speech policy. The company explained that the post would remain accessible because of its newsworthiness. As reported by the Wall Street Journal, the decision came from CEO Mark

Zuckerberg himself. This and similar decisions led one newspaper editor to call Zuckerberg "the world's most powerful editor."

As Chander outlined, this power to shape available speech on a key Internet platform establishes an odd relationship between privately created CGs and publicly enacted law. Conceived as a Venn diagram, he said, this relationship could go one of three ways: CG could prohibit only a subset of the speech prohibited by law; law could prohibit only a subset of the speech prohibited by CG; or the circles representing law and CG rules could overlap—with each set of rules prohibiting some content that the other permits. Pressures on platforms, governments, and Internet users vary depending on this configuration.

The company representatives expanded on this relationship, discussing the role of law and CGs in their internal practice. As described by Stern, national law becomes relevant to Facebook's content removal decisions only in cases where the law prohibits more speech than the CGs do. The company's first step is always to vet a removal request against the CGs. Only if the CGs do not require removal does Facebook proceed to consider national laws—looking to questions like the nature of the issuing authority, due process, and whether the order is directed to the creator of the content. This is a rigorous process, he said. Where national law truly requires removal, the company attempts to be "noisy" about compliance, and blocks the content only in that country. Describing Google's process, Downs emphasized that CG and legal removals follow separate internal tracks. For national law violations, Google, too, removes content for specific countries rather than the entire world.

Another question raised by Chander focused on the connection of CGs to civil law. In particular, he asked whether CGs set forth in companies' Terms of Service are binding contractual terms, enforceable through civil litigation. As he noted, if national courts enforced CGs to *mandate* removal of lawful content, this would create a troubling role for the law in delegitimizing and prohibiting lawful speech. This function of the law would be particularly concerning if the risk of civil damages led platforms to preemptively remove users' posts. On the other hand, problems might arise if the law *prevented* platforms from removing content based on their CGs. A key US intermediary liability law, Communications Decency Act 230, was enacted precisely in order to encourage platforms to take down content they deem inappropriate. As Chander explained, Congress enacted the law in response to a case that effectively punished an early platform for trying—but failing—to enforce CGs against offensive and defamatory speech. Fearing that the ruling would discourage platforms from voluntarily removing offensive material, Congress spelled out immunities for platforms that did so, as well as immunities for platforms that leave user content online. As a result, Chander noted, US law would be unlikely to support either mandatory CG "take-downs" or mandatory "leave-ups."

An audience question tied this analysis to questions of jurisdiction and national legal difference. If CGs are actually contractual provisions under platforms' Terms of Service, does that mean that CGs are subject to interpretation by national courts? As several speakers pointed out, the Terms of Service themselves are drafted to preclude this outcome, reserving ultimate discretion to the platforms. However, given national differences in consumer protection and contract law, such reservations of authority may not be enforceable in all countries. Grounding CGs in the

Terms of Service, and exposing them to national contract enforcement, could effectively reintroduce local legal variation and undermine the global effect of CGs.

Turning from civil law to criminal law, Llansó walked the audience through the increasing importance of CGs as a tool for national law enforcement. As she explained, counter-terrorism police units known as "Internet Referral Units" (IRUs) have been established in some EU countries and Interpol. IRUs review online content, identify material that is potentially terrorism-related, and report it to platforms for removal based on the platforms' CGs. One law enforcement officer publicly noted that relying on CGs—and not national law—is advantageous, because it allows police to seek removal of information that is not actually illegal.

As Llansó noted, IRUs have faced extensive criticism from civil society organizations. Many question whether using State resources and power to silence lawful speech is appropriate—or even consistent with constitutional and human rights of Internet users. Other critics have expressed alarm about law enforcement relying on private enforcement by platforms to effectively bypass national courts. When platforms resolve difficult questions about the balance between speech rights and public safety, societies may miss out on the important public conversations and policymaking needed to grapple with these very issues. Similar concerns arise, Llansó noted, regarding another important recent development: the 2016 Hate Speech Code of Conduct agreed on by the European Commission and four major platforms. As explained by Llansó, the Code of Conduct requires platforms to prohibit violent or hateful content under their CGs, and to accept removal requests on that basis. This too, she said, is an exercise of State power that causes private actors to suppress lawful speech.

In Llansó's analysis, even if much of the affected speech were actually unlawful, these programs would still raise an issue of users' rights to remedy and "oversight at scale." Errors by law enforcement or platforms are inevitable—but it is unclear what redress users have if the error came from enforcement of discretionary CGs. Transparency about law enforcement and platform removal efforts, and access to appellate review, are key to protecting users' rights. Remedies may be particularly important given the global scope of CG removals, which effectively amplify one country's law enforcement actions to users around the world.

> ***Does the Chinese model tell us that nations can have their cake and eat it too—maintain a bordered, regulated Internet without sacrificing a flourishing Internet commercial sector?***

Min Jiang identified a similar shift toward "voluntary" platform content removal in China. There, she said, content removal is increasingly initiated by platforms themselves, rather than government. The mesh of laws and operating licenses governing their operations give platforms strong incentives to internalize law enforcement goals and proactively remove potentially illegal information. At the same time, Jiang said, legal authority is often highly fragmented among different government actors and sources of law. A vast array of overlapping national and regional authorities have some say over Internet content issues. In addition, many of the most

important laws come from local regulation or other "lower level" sources of law—with only about ten percent of relevant law for platforms coming from sources like statutes, national regulations, or court decisions.

In addition, China famously has preserved bordered Internet access for citizens, using the "Great Firewall" and other technical and legal tools. Jiang explained the Chinese Internet of today as the product of a long and deliberate government policy of "Internet sovereignty." As early as 1995, the Chinese telecommunications minister stated the country's intention to preserve territorial borders online, comparing online communication to international travel: when you cross borders, you must go through customs, show your passport, and abide by national laws. "There is no contradiction at all," he wrote, "between the development of telecommunications infrastructure and the exercise of State sovereignty." Following this policy, China has, in Jiang's words, "painstakingly grafted borders onto the Internet."

A striking feature of the Chinese story, Jiang pointed out, is the economic success of Chinese Internet companies in recent years. Does the Chinese model tell us that nations can have their cake and eat it too—maintain a bordered, regulated Internet without sacrificing a flourishing Internet commercial sector? This question may become all the more pressing given, as other conference participants pointed out, the apparent interest of Russia and other countries in following a similar path.

In her closing remarks, Jiang described a shift toward a "re-nationalized," bordered Internet – with erosion of liberties and increasing surveillance and filtering of online communications. As she noted, this trend is by no means limited to China. Lawmakers around the world are increasingly troubled by online content that violates their laws, and increasingly aggressive about enforcement. A similar observation was voiced by Google's Juniper Downs. Describing her own conversations with governments, she observed "a real inflection point" regarding platforms' role in policing user-generated content. Andrea Glorioso of the European Commission, who was participating in his personal capacity, weighed in from the audience to echo the observation. The Internet industry, he said, severely underestimates the emerging climate of localism in both the EU and the US. The internationalism that has long characterized Internet policy is waning, and the demand from national governments for Internet companies to solve problems created by online content is growing.

> ***If the alternatives are "harmonization" of national laws via private platforms' Terms of Service, or an increasingly bordered and fragmented Internet governed by national laws, which do we actually prefer?***

This shift in government and public expectations is importantly connected to platforms' voluntary enforcement of CGs as a basis for removing online content. Are CGs the new de facto

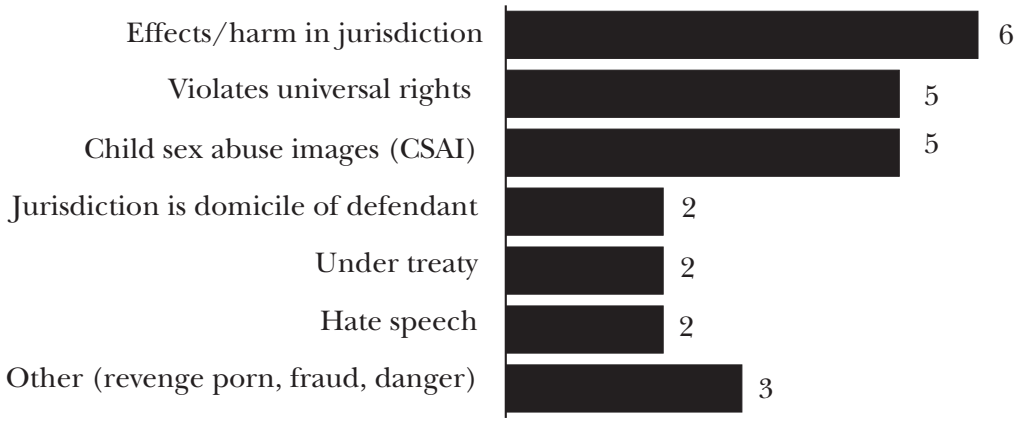
source of international norms – resolving regional differences not through transnational cooperation of governments, but through unilateral action of private companies? If platforms' choices are not truly unilateral but shaped by pressure from powerful State actors, should that raise concern about extraterritorial action by national governments? If the alternative to "harmonization" of national laws via private platform CGs is an increasingly bordered and fragmented Internet, which do we actually prefer? Our evolving answers to these questions will determine the real-world power of State and private actors, and the real-world choices of Internet users seeking information or exercising expression rights online, in the coming years.

Appendix 1: Survey Results

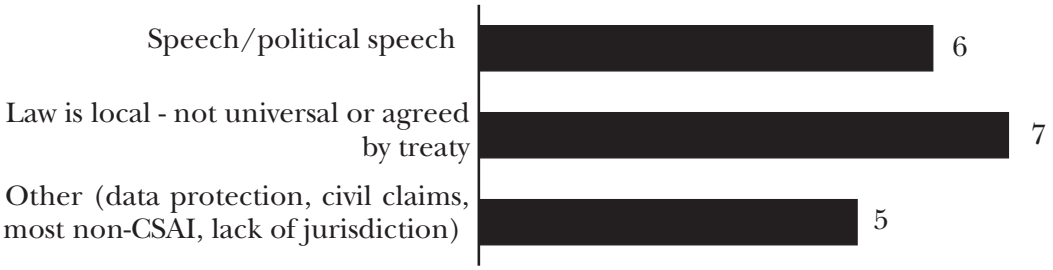
As part of the conference's closed session with invited participants, CIS circulated a survey. The results are below. These draw on a relatively small sample – just 21 people – each with expertise in online jurisdiction issues. The responses are illuminating both for the points of relative consensus and those which generated very little agreement.

For the questions shown on pages 45-47, participants wrote answers in their own words. We grouped similar responses (such as "universal rights" and "human rights") as the same for purposes of our count. Even so, many questions elicited widely varying responses. The widest variation related to blackletter doctrine and geoblocking. For those topics, we have reproduced answers verbatim.

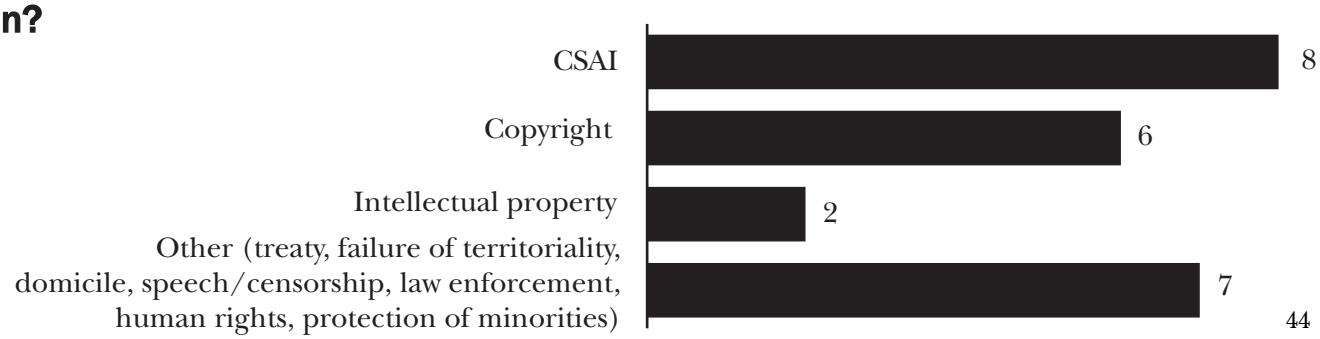
In what situations, or for what kinds of legal claims, is it most appropriate to order extraterritorial deletion?



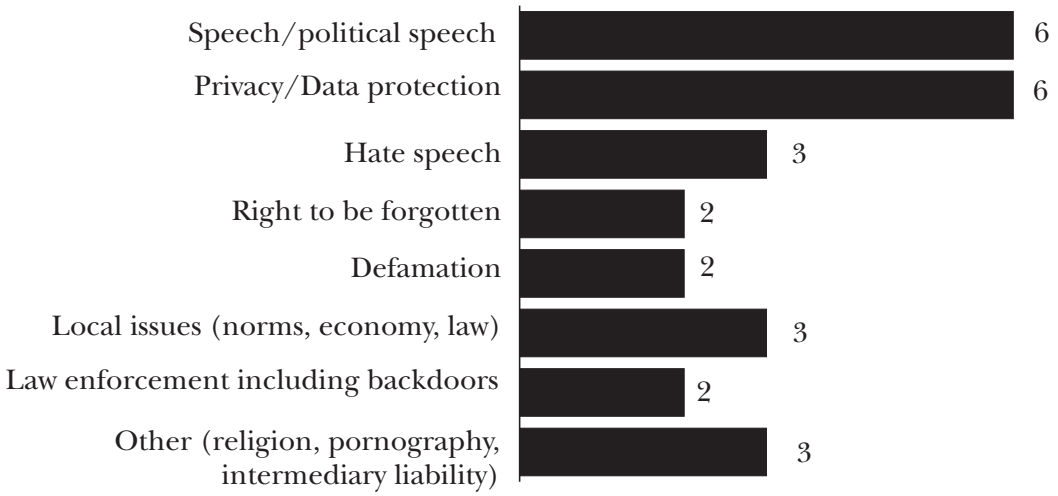
In what situations, or for what kinds of legal claims, is it least appropriate to order extraterritorial deletion?



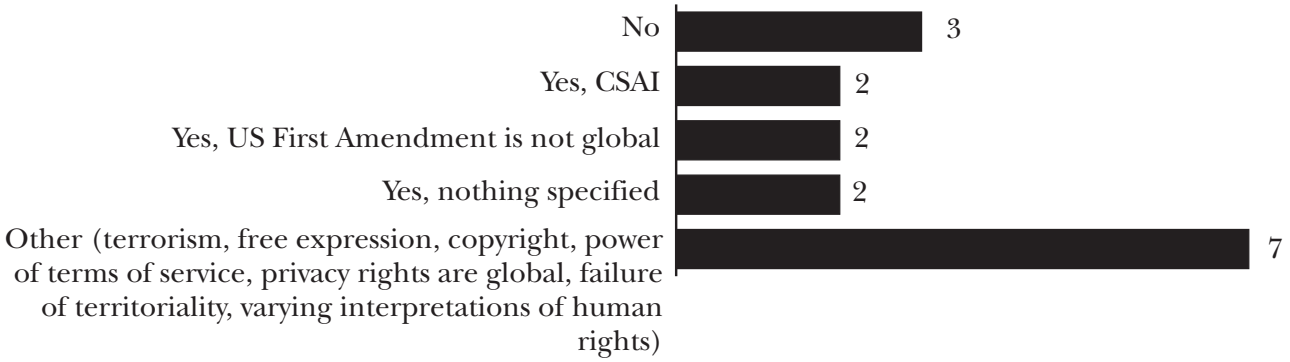
Of the legal issues discussed in the conference, what topics are different national governments around the world most likely to agree on?



Of the legal issues discussed in the conference, what topics are different national governments around the world least likely to agree on?

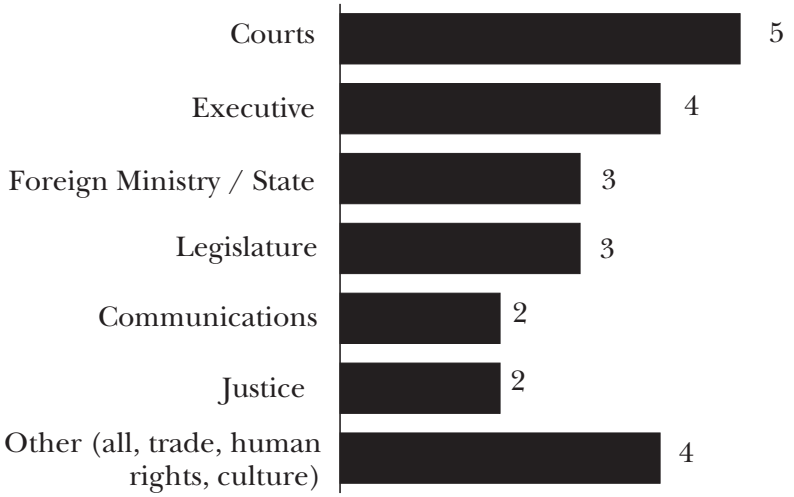


Do you see emerging consensus on any of these issues among other groups of stakeholders (companies, civil society, etc.)? If so, what?



In plaintiff's country, what branches of national government should be most interested and concerned when courts in one country order deletion of content in another?

In defendant's country, what branches of national government should be most interested and concerned when courts in one country order deletion of content in another?



Do you believe international agreement among countries on issues of jurisdiction and choice of law for Internet content removal is possible? By what year?

Do courts have the doctrinal tools they need to resolve cross-border deletion requests? If not, what would help?

Yes 4

> Willingness to defer to congruent rules made by non-governmental polities.

> Local law.

> Do they come before courts? In the UK, only for piracy and trademark.

> If they consider/apply international norms; yet respect sovereignty with limits.

No 12

> A modern articulation of comity factors. Online cases should not be viewed as locations, and need new factors such as global impact and human rights.

> Standard for determining whether a judicially mandated or court supervised document is sufficient for due process and rule of law.

> A clear legal analysis of extraterritoriality as it relates to jurisdiction.

> Multilaterial international human rights consensus.

> A new jurisprudential framework for jurisdiction.

Is geoblocking in response to national laws an emerging norm for online publishers and intermediaries? If so, does that raise any concerns for you?

Yes 12

> User choice. Withholding content that's lawful in the jurisdiction. Cost for small companies to implement.

> The fragmentation of the Internet. Balkanization.

> Wikimedia is not divided by country, but by language. Speakers of some languages span many places with wildly varying laws.

> Silent censorship. Extraterritorial jurisdiction. Collateral damage.

> I think there is something of a technical burden on smaller companies as geoblocking advances.

> Huge ambit for abuse. Blunt instrument.

> Disruption of the ideal of free end to end connection.

> The best solution that we have, in balancing respect for national laws in countries when the company has subjected itself to jurisdiction with a general commitment to promote free expression and access to information. But it also depends on companies being very careful about which countries they enter.

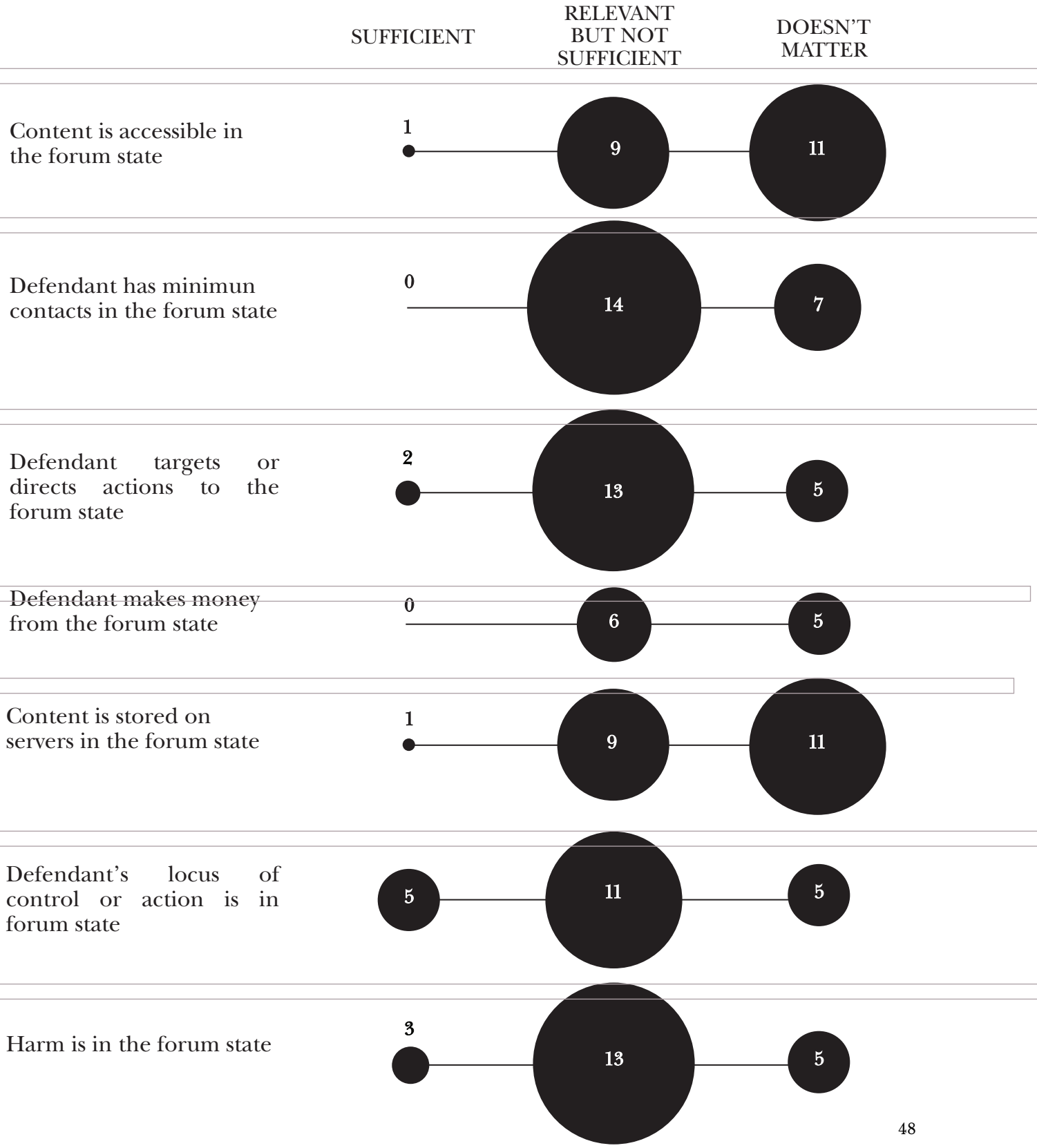
No 4

> It seems it is not seen as enough, compared to global blocking, and this is a concern.

> Fragmentation of cyberspace but this is already happening in terms of localized products.

> A clear legal analysis of extraterritoriality as it relates to jurisdiction.

What activities by an online publisher or intermediary defendant should suffice for a court to order the defendant to delete or de-list content outside of the forum state's territory?



Appendix 2: Hypothetical Situations for Group Discussion

The second, closed day of the Law, Borders, and Speech Conference included a lively debate about the following three hypothetical scenarios. We are sharing them in hopes that others may find them equally provocative and useful. They are generally based on real life, but include significant simplifications, changes, or fact patterns invented for the purpose of the exercise.

Internet Platforms

Hypo 1: Anne Frank and Wikipedia

Wikimedia receives a DMCA removal request from the US copyright holders for The Diary of Anne Frank, demanding that Wikipedia remove all links to, or hosted copies of, the original Dutch-language version of the diary. The diary is in the public domain under Dutch copyright law, but still protected by US copyright law. Wikimedia is legally established in the US, and its employees and servers are all here. It has separate Dutch and English-language pages about the diary, and allows users to navigate to either one. Both the Dutch and English pages have links to a Wikimedia-hosted copy of the diary at the time the DMCA request arrives. What should it do in response to the request?[15]

Hypo 2: Reddit and Russia

In 2013, Russian regulator Roskomnadzor ordered Russian ISPs to block a page on reddit.com where Russian users discussed illegal drugs. Because Reddit encrypts traffic using HTTPS, the ISPs could only block the entire site—not individual pages. Russia later agreed to lift the ban, and Reddit agreed to block traffic at its end by preventing users with Russian IP addresses from accessing pages that violate Russian law. This allowed the rest of Reddit to remain accessible in Russia.[16]

Suppose that Roskomnadzor notifies Reddit that another page violates Russian law. This one offers psychological support for gay and transgender teenagers in Russia. Russian regulators say, and local counsel in Russia confirms, that the page violates Russia's "gay propaganda" laws. What should Reddit do now?

Hypo 3: DuckDuckGo and the EU

[15] These facts are simplified based on the real world example described here. Among other differences, the public domain status of the diary in the Netherlands is disputed in real life.

[16] Up to this point the hypo tracks reported facts.

DuckDuckGo is a search engine company based in Pennsylvania. It prides itself on protecting users' privacy by not tracking them.

The company has no offices, employees, or servers outside the US, and it does not deposit cookies on users' machines. It does sell advertising space in search results, including to advertisers in the EU. It allows ad campaigns to target users in particular countries or regions, presumably based on the user's IP address. It also lets users create accounts in order to participate in discussion forums, including forums for open source developers who contribute code to the search engine. It supports informal in-person "Quack & Hack" meetings for these developers, including in the EU. The Strasbourg Quack & Hack group, for example, has 98 members. According to alexa.com, at least 23% of DuckDuckGo's traffic comes from users in the EU.

The EU's pending General Data Protection Regulation, which goes into effect in 2018, arguably applies to DuckDuckGo because of the accounts it maintains for EU users. French Counsel has advised the company that the law is unclear, but she thinks there is a 40% chance that regulators and courts would find jurisdiction to apply the law to the company. If that happens, DuckDuckGo would face some expensive legal and technical compliance work, and also have to honor "Right to Be Forgotten" requests for search results. French regulators maintain that such de-listings must apply globally, not just to results seen by European users. The search engine currently does not honor such requests, which means that European users can use DuckDuckGo to find results that Google has de-listed.[17]

Suppose that in October 2018, the CEO of a French shipping company threatens to sue DuckDuckGo if it does not de-list search results linking to allegations that he cheated on his taxes ten years ago. The French Data Protection Authority agrees that he has a right to de-list the results. What should DuckDuckGo do now?

[17] Facts up to here are based on reporting by DuckDuckGo and other Internet sources – though not always clearly reliable ones, so take these details with a grain of salt. Main exceptions: (1) in real life, DuckDuckGo partners with Bing and Yahoo for ads and results; (2) we made up the legal prediction about odds of French lawmakers finding jurisdiction over DuckDuckGo.

Appendix 3: Glossary: Internet Content Blocking Options and Vocabulary

Daphne Keller

Conversations about unlawful online content and the responsibilities of Internet intermediaries have become more heated in recent years. Participants in these discussions often lack common terminology or understanding of technological options for online content control.

This problem is not entirely new—there has never been a single agreed set of terms, and people have often used the same terms to mean different things. But miscommunications become more consequential as governments expand legal mandates for intermediaries. Different blocking technologies lead to different outcomes, which can include under-blocking unlawful content, over-blocking lawful content, or disrupting service to users. They can also place different burdens on intermediaries, and make it easier or harder for users to circumvent the blocks or for researchers to detect them.

This document briefly lists key terms as the author has seen them most commonly used. It also lists common sources of confusion.[18]

I. Common Terms

Intermediaries: Entities that "give access to, host, transmit and index content originated by third parties or provide Internet-based services to third parties."[19] There are many kinds of intermediaries, but for purposes of content blocking or removal they can generally be clustered into two groups with different capabilities.[20]

- *Network intermediaries*, which provide technological connections between two endpoints, can sever that connection. (Examples: ISPs, mobile carriers, content delivery networks, and DNS providers.)
- *Hosting intermediaries*, which store user content on their servers, can remove content or restrict access to it. [21] (Examples: consumer-facing hosts such as Facebook, back-end hosting providers such as Amazon Web Services.)

---

[18] Joe Hall and Jim Greer kindly checked this for errors. If I introduced any after their review, it's my fault.

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

[20] End-to-end design principles would suggest moving blocking capabilities away from these intermediaries and toward the edges of the network—for example, by enabling blocking at the level of an individual user's mobile phone or browser. *See* Larry Lessig, *The Future of Ideas* (2001) pp. 34-39; *Cyberspace's Architectural Constitution* (1999) https://cyber.harvard.edu/works/lessig/www9.pdf.

[21] For purposes of content blocking and removal, a search engine or other entity providing links to content functions like a host. Removing a link typically means removing hosted HTML. For search engines, it may include page title, snippet text, the link itself, and cache copies of webpage.

Content Providers: "[T]hose individuals or organizations who are responsible for producing information in the first place and posting it online."[22]

Remove or take down: To erase or restrict access to online content, in whole or in part.

Block: To prevent a user from accessing content, without taking the content itself offline.

- *Variations in the blocking target:* Sometimes intermediaries block particular *content* (like when an ISP stops all its users from going to a website or using an app). Sometimes they block particular *users* (like when a website blocks all users with IP addresses from a certain country). Sometimes they do both at once (like when Twitter prevents users in a particular country from seeing a particular tweet—which they call *withholding* content).

- *Variations in the blocking implementation:* An intermediary can block content completely, or can do more subtle or complex things like degrading service (as can happen to foreign websites passing through the "Great Firewall of China"), demoting content visibility (as Google web search has done on DMCA grounds), removing content but notifying users who try to access it that it was removed (as WordPress does for DMCA removals), warning users before they choose to view content (as the Blogger platform does for adult content), or even supplementing offensive content with additional context or counter-speech (as Google did in response to the 2004 "jew watch" controversy, and Jigsaw has done with newer tools).

- *Variations in the means used to identify information for blocking:* In order to block users or content, an intermediary must have a way for machines to identify which Internet communications are to be blocked.
    - *Users* may be blocked based on *identifying information* such as an account, or *location information* such as an IP address.
    - *Content* is most commonly blocked based on its *location*. Intermediaries can block based on a web URL (like www.example.com for an entire site or www.example.com/page for a single page)[23] or an IP address (like

[22] Article 19, *Internet Intermediaries: Dilemma of Liability* (2013) at 6, https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf. For some purposes, such as copyright, the law must also distinguish between original authors and those who merely re-post information.

[23] "URL-based blocking compares the website requested by the user with a pre-determined "blacklist" of URLs of objectionable websites selected by the intermediary imposing the blocking. URLs (or uniform resource locators, otherwise known more colloquially as "web addresses") are character strings that constitute a reference (an address) to a resource on the internet and that are usually displayed inside an address bar located at the top of the user interface of web browsers." Angelopolous et al, *Study of fundamental rights limitations for online enforcement through self regulation* (2016) https://www.ivir.nl/publicaties/download/1796, at 7.

216.3.128.12).[24] In some cases they can disrupt elements of the Domain Name System in order to prevent a URL from resolving to the correct IP address.[25] Location-based blocking can be over-inclusive (like by blocking all content on an IP address, when only some of it is unlawful) and under-inclusive (like by blocking one instance of an MP3 file, when identical copies exist at other locations).
    - Intermediaries can also block based on *technical specifications* (such as blocking a port to prevent use of VOIP).
    - Most ambitiously, intermediaries may block by building software capable of recognizing *specific content*. *See* "*Filter", below.*

- Websites that protect their users through SSL encryption (indicated by "HTTPS" in the browser address bar) may suffer unintended consequences if network intermediaries attempt to block content on the site. With SSL in place, an ISP monitoring user traffic may only be able to identify the site being accessed (www.example.com)—not the individual page (www.example.com/page) or any of its content. As a result, an ISP's only options may be to block an entire site, including huge sites like youtube.com or wikipedia.org, or to block none of it.[26]

Monitor: To review online information with the goal of identifying specific, usually objectionable content. Automated monitoring tools look for particular content, such as an image or a phrase.

Filter: To take "action against material identified through monitoring in order to then block access to it or remove it[.]"[27] Tools that hosting intermediaries can use to filter content include

---

[24] "This operates in a similar manner to URL blocking, but uses IP (Internet Protocol) addresses, i.e., the numerical labels assigned to devices, such as computers, that participate in a network that uses the internet protocol for communication. IP-based blocking has a higher chance of resulting in unintended 'over-blocking' than targeted URL blocking as a result of IP sharing, as a given unique IP address may correspond to multiple URLs of different websites hosted on the same server." Angelopolous et al at 7.

[25] There are many variants on DNS disruption, ranging from DNS seizures (which break DNS resolution for users globally) to DNS disruption by ISPs, which affect only their users.

[26] The distinction between "location" and "content" can be fuzzy – very much as the distinction between "metadata" and "content of communications" is fuzzy in the surveillance context. For example, a URL designates location, but can also tell you something about the content of the page. (Example: www.example.com/donaldtrump.htm).

[27] "Monitoring tools such as content control software can be placed at various levels in the internet structure: they can be implemented by all intermediaries operating in a certain geographical area or only by one or some of those intermediaries; they can be applied to all of the customers of an intermediary or only to some of them (for example only to customers originating form country X); they can look only for certain content which is commonly transmitted through specific services (such as illegal file sharing through peer-to-peer networks) or indiscriminately to all content." Angelopolous et al at 6. In order to effectively catch specific content, monitoring must be "systematic, universal, and progressive." AG Cruz Villalon in SABAM Opinion, quoted in Angelopolous et al.

keyword blocklists,[28] PhotoDNA for duplicate images,[29] AudibleMagic for duplicate audio tracks,[30] or YouTube's ContentID for duplicate video.[31] They can also use human monitors, or a combination of technical and human monitoring. For ISPs, it is sometimes possible to identify and block content using Deep Packet Inspection (DPI), but this is computationally expensive. Content-based blocking is often costly. The risk of over- or under-inclusion—of blocking too much or too little—varies substantially depending on kind of technology, content, and legal claim at issue.[32]

Geolocate: to determine the location of a device, typically a user's computer or mobile phone. This is typically done using IP address, GPS, WiFi network identification, or other technical information.

Geoblock: to use geolocation data to block particular devices or users (like Reddit blocking Russian users from certain pages).

II. Sources of Confusion

Miscommunication about removal issues often involves one of the following questions.

1. Is the intermediary a network intermediary, or a hosting intermediary?

This matters, because network intermediaries can block the channel of transmission, preventing users from reaching content (example: ISP blocking an IP address). Hosting intermediaries, on the other hand, can take content offline completely (example: YouTube removing a video based on a DMCA request). *See "Intermediaries" definition, above.*

2. How is the intermediary identifying information to block?

The technological means for blocking content are rarely perfect. Many blocking mechanisms foreseeably lead to specific types of over- or under-blocking. Blocking an IP address, for example, prevents users from accessing any lawful material that shares an IP address with the targeted content. Blocking a specific webpage may be ineffective if the webmaster merely re-posts the same content on a different part of the site. Filtering tools like ContentID that identify duplicate content may fail to recognize modified copies on the one hand, or erroneously remove

---

[28] Keyword blocking typically involves identifying words or strings in static online content. Over-removal issues with keyword blocklists of this sort are well illustrated in the Wikipedia entry for the Scunthorpe Problem, https://en.wikipedia.org/wiki/Scunthorpe_problem. Intermediaries can also keyword block text submitted by users – for example, a search engine might show no results if a user searches for "Tiananmen."

[29] https://en.wikipedia.org/wiki/PhotoDNA

[30] https://www.audiblemagic.com/

[31] https://support.google.com/youtube/answer/2797370?hl=en

[32] See, e.g., http://www.engine.is/the-limits-of-filtering.

satire and other lawful use on the other. *See "Variation in the means used to identify information for blocking," above.*

3. Is "bad" content completely deleted, or does something else happen?

Removal can be partial and incomplete in various ways. For example, intermediaries can deny access to content for just some users (based on location, age, etc.), or some user activities (such as searching for certain specific names on Google under "Right to Be Forgotten" laws). An intermediary can also demote certain content (putting it lower in search results or a news feed), degrade connection speed (making it hard to load a page or watch a video), or otherwise deter users from accessing it (such as through a malware warning or fake news label). To my knowledge, there is no good umbrella term that encompasses all these options. *See "Variations in the blocking implementation," above.*

III. Other Sources of Information

- https://www.internetsociety.org/doc/internet-content-blocking
  Excellent and up-to-date re network intermediaries; not comprehensive re hosting intermediaries.

- https://tools.ietf.org/html/draft-hall-censorship-tech-04
  Excellent and recent, great citations, somewhat technical. (Per IETF practice, "expired" as of January 2017 and not to be cited, but future version may be released as RFC.)

- http://access.opennet.net/wp-content/uploads/2011/12/accessdenied-chapter-3.pdf; https://opennet.net/about-filtering
  Technically good but probably drafted ten years ago and some terminology does not match current normal use. (Project was launched in 2004, shut down in 2014.)

Appendix 4: Recommended Readings

Cases

- Google and Commission Nationale de L'Informatique et des Libertés (CNIL) ("Right to Be Forgotten" case)
  - Conseil d'Etat ruling
  - CJEU ruling expected 2018
- *Google Inc. v. Equustek Solutions Inc.* (fka *Equustek v. Jack*)
  - Ruling, Supreme Court of Canada, 2017
  - Amicus briefs listed under "Intellectual Property Law" and "Human Rights Law," below
  - CIS blog post and Graham Smith post on Canadian ruling
  - CIS blog post on US challenge to Canadian ruling
- *X v. Twitter*, New South Wales Supreme Court, Australia, 2017
- *EFF v. Global Equity*, US District Court, 2017
- *eDate/Martinez*, CJEU, 2011
- *Pammer/Alpenhoff*, CJEU, 2010
- *Pinckney v. Mediatech*, CJEU 2013
- LICRA v. Yahoo! ("Yahoo France" case)
  - Ruling, Superior Court of Paris, 2000
  - Ruling, US District Court, 2001
  - Ruling, US Circuit Court en banc, 2006
- Gutnick v Dow Jones & Co Inc., High Court of Australia, 2002

Big Picture

- David R. Johnson and David G. Post, Law and Borders - The Rise of Law in Cyberspace. Stanford Law Review, Vol. 48, p. 1367 (1996)
- Bertrand de la Chapelle and Paul Fehlinger, Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation, commissioned by the Global Commission on Internet Governance
- David G. Post, Internet Infrastructure and IP Censorship
  - Summary
  - Full PDF
- David R. Johnson and David G. Post, 'Chaos Prevailing on Every Continent': Towards a New Theory of Decentralized Decision-Making in Complex Systems, 73 Chicago-Kent L. Rev. 1055 (1998)
- Uta Kohl, The Net and the Nation State, (2017) (for purchase)

Geoblocking Tools and the Law

- Joseph Lorenzo Hall, Center for Democracy & Technology
  - A Survey of Worldwide Censorship Techniques
  - Technology Behind (Geo)Blocking
- Marketa Trimble
  - The Role of Geoblocking in the Internet Legal Landscape, IDP, Revista de Internet, Derecho y Política (23) (2017)
  - Geoblocking and Evasion of Geoblocking – Technical Standards and the Law, in GEOBLOCKING AND GLOBAL VIDEO CULTURE (Ramon Lobato & James Meese eds., Institute of Network Cultures, Amsterdam) (2016)
  - The Territoriality Referendum, 6 WIPO J. 89 (2015)
  - Future of Cybertravel: Legal Implications of the Evasion of Geolocation Fordham Intellectual Property, Media & Entertainment Law Journal, Vol. 22 (2012)
  - To Geoblock, or Not To Geoblock – Is That Still a Question?
  - Your Movements Shall Be Traced: The New EU Regulation on Cross-Border Portability
- Internet Society, Perspectives on Internet Content Blocking: An Overview
- Steven J. Murdoch and Ross Anderson, Tools and Technology of Internet Filtering
- OpenNet Initiative, About Filtering

Intellectual Property

- *Equustek* brief of Electronic Frontier Foundation
- *Equustek* brief of FIAPF (Fédération Internationale des Associations des Producteurs de Films)
- *Equustek* brief of IFPI (International Federation of the Phonographic Industry)

Data Protection and the Right to Be Forgotten

- Decision no. 2016-054 of March 10, 2016 of the Restricted Committee issuing Google Inc. with a financial penalty. Authored by Commission nationale de l'informatique et des libertés
- Michel Jose Reymond, Hammering Square Pegs into Round Holes: The Geographical Scope of Application of the EU Right to Be De-listed Berkman Klein Center Research Publication No. 2016-12 (2016)
- Brendan Van Alsenoy and Marieke Koekkoek, Internet and jurisdiction after *Google Spain*: the extraterritorial reach of the 'right to be de-listed', International Data Privacy Law, Volume 5, Issue 2, Pages 105–120 (2015)

Human Rights Law

- *Equustek* brief of Human Rights Watch, Article 19, Open Net (Korea), Software Freedom Law Centre and Center for Technology and Society
- Evelyn Aswad, The Role of US Technology Companies as Enforcers of Europe's New Internet Hate Speech Ban

Law Enforcement Access to User Data

- Albert Gidari MLAT Reform and the 80 Percent Solution
- Andrew K. Woods and Jennifer Daskal, Cross-Border Data Requests: A Proposed Framework
- Andrew K. Woods and Jennifer Daskal, Congress Should Embrace the DOJ's Cross-Border Data Fix
- Proposed UK-US MLAT legislative change to forego MLATs and to permit direct disclosure of content to UK authorities
- GDPR Art. 48: "Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter."
- Regulation of Investigatory Powers Act 2000

Black Letter Law

- Dan Svantesson, A doctrine of 'market sovereignty' to solve international law issues on the Internet? 2014
- Dan Svantesson, A Third Dimension of Jurisdiction, 2015
- Dan Svantesson, Solving the Internet Jurisdiction Puzzle, 2017 (for purchase)

Real Power, Real Outcomes, Realpolitik

- Backpage.com v. Dart - 7th Circuit Court of Appeals decision
- CDT's amicus brief in Backpage.com v. Dart
- The rule of law on the Internet and in the wider digital world, Council of Europe Commissioner for Human Rights
- European Commission Hate Speech Code of Conduct
- CDT letter to Commissioner Jourova describing concerns: https://cdt.org/insight/letter-to-european-commissioner-on-code-of-conduct-for-illegal-hate-speech-online/
- Commissioner Jourova response

- ARTICLE 19 analysis of Code

Other Projects

- Internet & Jurisdiction Policy Network
  - Project Page
  - Content and Jurisdiction Policy Options
  - Retrospect Database of news and developments
- Geneva Internet Disputes Resolution Policies 1.0, Topic 1: Which national courts shall have jurisdiction in Internet-related disputes?

Appendix 5: Speaker Presentations

Uta Kohl, Aberystwyth University

What happened to the 'presumption against extraterritoriality' in the online global order? A black letter tool to encourage jurisdictional restraint on the internet?

Today I want to talk about the presumption against extraterritoriality and why it has figured – rather paradoxically – very rarely in Internet cases and but why it may after all be a useful tool to encourage the coexistence of territorial state law on the internet through mutual restraint. Let me start with Hannah Buxbaum's ideas on territoriality and extraterritoriality. She says: '"Territoriality" and "extraterritoriality"… are legal constructs. They are claims of authority, or of resistance to authority that are made by particular actors with particular substantive interests to promote.'[33] In other words, territoriality (or territoriality of law and order) is not a 'natural' state of affairs, but a legal construction created to protect certain interests and resisted by others. Furthermore and however ill-suited it may be for the global (online) market place, territoriality remains the norm or the default standard for legitimate authority. By the same token, 'extraterritoriality' is something outside the norm and carries with it a strong whiff of illegitimacy. So, actors in cross-boundary disputes – whether individuals, corporations or States – invariably invoke the concept of extraterritoriality to assert that a state has gone *beyond* its authority. That very contest between legitimate and illegitimate authority also strongly (albeit not completely) underlies the presumption against extraterritoriality, which in its very essence embodies the exceptionality of extraterritoriality.

Before coming to this, however, let me briefly reflect on the drivers behind jurisdictional contests. Partly, undoubtedly, they are driven by cultural and political diversity or the desire of each State to uphold its collective notion of the 'good life' within its borders and for its population. That desire then makes it clear why extraterritorial overreach is often delegitimised by invoking human rights, in particular free speech. One State's effort to control information flows in accordance with its own political priorities often impacts on the free uninhibited information flow elsewhere. This view is undoubtedly a valid perspective for many of the Internet jurisdiction disputes. Yet, not all. Many Internet jurisdiction disputes may more usefully be constructed as free trade cases, rather than free speech contestations (even if they have speech implications) in order to understand their underlying dynamics. A clear-cut example lies in the cross-border online gambling regulation by the US which is intended to protect its local gambling industry from foreign online competitors. However, there are also more

[33] Hannah L Buxbaum, 'Territory, Territoriality, and the Resolution of Jurisdictional Conflict' (2009) 57 AM. J. COMP. L. 631, 635

ambiguous cases which are driven by economic interests that have speech repercussions, such as trademark/domain name disputes or even data protection actions. Typically, the Spanish claimant in the EU "Right to Be Forgotten" case relied on data protection to protect his 'informational self-determinacy' which in turn was designed to protect his business as a solicitor. Data is a valuable commodity, the most valuable we have today, and the CJEU with its judgment pushed some of that value back from Google to the European user. Should the extraterritoriality of the ruling be understood and/or challenged on the basis that it is inconsistent with free speech (as understood outside but not within Europe) or as European *economic* protectionism? This is something worth pondering.

Coming to the presumption against extraterritoriality, most of you, if you are lawyers, will be familiar with it from your first year in law school, as a basic tool of statutory construction. But if you are not a lawyer and you are the 'man on the Clapham omnibus' (as we would say in the UK), you know the presumption without knowing that you know it; it's popular wisdom and deeply embedded in the social imagination. It is that France has a right to regulate what occurs on French soil and not beyond, unless there are exceptional circumstances, and the same applies to every other country. And this is exactly what the presumption against extraterritoriality provides: legislation applies to persons and matters within the territory of the State, but not to persons and matters outside the territory, unless the legislation evinces a contrary intention.

The presumption is applied by the judiciary to interpret the territorial application of legislation, making the assumption that, bar exceptional circumstances, a national parliament would not try to regulate outside its borders. So, here the presumption applies to substantive law, be it criminal, regulatory or civil. In the 2004 US antitrust case of F. Hoffmann-La Roche Ltd v Empagran S.A.,[34] the Supreme Court applied the presumption against extraterritoriality to the Sherman Act, holding that foreign conduct causing foreign harm lay outside the mischief the Act sought to remedy. More recently, the presumption has also been applied to judicial jurisdiction; here it does not limit the effect of the substantive law, but the competence of local courts to hear certain claims. In 2013, in Kiobel v Shell,[35] the Supreme Court held that the presumption against extraterritoriality applied to the Alien Tort Statute, which had led to much human rights litigation against multinational corporations, and restricted judicial competence under that statute to those matters that have a strong connection with the US.

What does the presumption seek to achieve? It advocates caution and restraint in extraterritorial regulatory assertions, saying that in the vast majority of cases it is inappropriate to extend the law and litigation to matters that lie outside the State's territory. In other words, it does exactly what the ordinary man instinctively knows: stick to your borders. In Empagran the Supreme Court explained this caution by saying: 'This Court ordinarily construes ambiguous statues to avoid unreasonable interference with other nations' sovereign authority. This rule of construction reflects customary international law principles and cautions courts to assume that legislators take account of other nations' legitimate sovereign interests when writing American laws. It thereby helps the potentially conflicting laws of different nations work together in

[34] 542 US 155 (2004).
[35] 133 S.Ct. 1659 (2013).

harmony.' (emphasis added) The Court then explained that the comity concern remains real insofar as other nations may not have adopted antitrust law similar to the US or, even if they had, they may 'disagree dramatically about appropriate remedies.' The presumption is driven by the potential conflict of different laws and in recognition of each nation's sovereign authority and the desire for harmonious global working order. Of course, it is only a presumption and can be set aside by appropriate evidence. Extraterritoriality may be 'reasonable, and hence consistent with principles of prescriptive comity, insofar as [the laws] reflect a legislative effort to redress domestic antitrust injury that foreign anticompetitive conduct has caused.'

Now let us think about the Internet cases where the presumption would appear to be highly pertinent, given that each State's regulation of online activity always has some extraterritorial effect. Yet, despite its intuitive relevance, the presumption has been almost entirely absent from the Internet governance debate and judicial jurisdiction reasoning. (A rare exception is the *Microsoft* case, but that case is not quite the standard internet jurisdiction scenario insofar as its deals with enforcement activity.) In the standard internet jurisdiction case, judges simply find that the foreign online content or service provider has to comply with local law on the basis that a local injury is caused or a local interest is affected by the foreign website or online activity. This approach means that the law and its application to the facts is either not treated as extraterritorial at all (i.e., we are only regulating what occurs in our territory) OR, alternatively, the presumption is displaced, along Empagran reasoning that the law's territorial overreach is justified as a legislative effort that simply seeks to redress a domestic injury caused by foreign conduct. Whilst from an internal, national perspective such reasoning seems quite reasonable, the presumption against extraterritoriality has an in-built global perspective; it recognises the interests of other States against the regulating States and the global interest in a global harmonious working order. So such internal perspective is out of kilter with the presumption's in-built aim.

Let us now have a look at Art 3 of the General Data Protection Regulation (GDPR)[36] which lays down the territorial scope of the EU data protection regime and is entirely consistent with the body of Internet jurisdiction cases (using 'jurisdiction' in the broad sense of involving the adjudicative and legislative competence of States). Through Art 3, the European legislator evinces an intention to apply the GDPR extraterritorially (i.e., a displacement of the presumption) in three different ways:

First, it applies the GDPR 'to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not' (Art 3(1)). This builds on the approach taken in Art 4(1)(a) of the *Data Protection Directive*,[37] as applied in *Google Spain*,[38] but makes it an express stipulation

[36] 2016/679; adopted on 27 April 2016, enters into force in May 2018.

[37] 95/46. Article 4(1)(a): 'Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary

that the location of the processing is irrelevant to the competence question, as long as the processing occurred 'in the context of the activities of an establishment of a controller.' So this approach gives legislative validation to the CJEU judgement in *Google Spain* that foiled Google's attempt to bring itself outside the EU regime by virtue of its non-EU-localised processing activities.

Second, Art 3(2) applies the GDPR 'to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the *processing activities are related* to: (a) *the offering of goods or services*, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) *the monitoring of their behaviour* as far as their behaviour takes place within the Union.' (emphasis added) So again the processing may well place outside the EU and the only connection with the EU needed are the (commercial) activities of the controller or processors. This Article throttles attempts to avoid the effect of Art 3(1) through not having an establishment in the EU whilst still doing online business in the EU, for example social networking or sharing economy websites. Although this Article purports to look at to whom the foreign web activity is in substance targeted, in fact it does not ask whether Europeans are a main or rather marginal target of the site and thus is hardly consistent with the 'targeting' or 'directing' approach that has been advocated as a more moderate approach to jurisdictional assertions.

Third, through Art 3(3), the GDPR is extended 'to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.' This last head is effectively a catch-all provision that allows for any cases to be brought within the GDPR that has not already been legitimised by the previous two heads. After all, public international law is highly permissive in terms of adjudicative/prescriptive jurisdiction, particularly in the form of a very flexible territoriality principle.

While Article 3 appears excessive in its extraterritorial reach, seeking to bring into its ambit everyone and anyone who deals, however marginally, with personal data of the 'data subjects who are in the Union', in fact its approach is unexceptional. It perfectly fits within the broad body of transnational Internet regulation through States, starting with various US cases from 1996, to *LICRA v. Yahoo!* in France in 2001 and *Gutnick*[39] in Australia in 2002, to the recent *Equustek Solutions Inc v. Jack*[40] in Canada. This body shows no sign of the restraint and caution that the presumption against extraterritoriality advocates in the name of the greater orderly global public good. The body makes extraterritorial regulation the norm rather than the exception on the basis that the formerly exceptional case of local injury caused by foreign conduct has become the norm. The default of State regulation is extraterritoriality in perfect unison with the default global reach of online activity.

---

measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.'

[38] *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (2014) Case C-131/12.

[39] *Gutnick v Dow Jones & Co Inc.* [2002] HCA 56.

[40] *Equustek Solutions Inc v. Jack* 2014 BCSC 1063. This presentation pre-dated the Canadian Supreme Court's subsequent decision, which affirmed the appellate ruling referenced here.

Whereas on a technical legal level the result of this position signals the effective expiry of the presumption, in broader regulatory terms the presumption reflects and embodies a global order based on State law and thus the presumption's non-viability is a marker of the non-viability of the State as an effective regulatory agent. Where everybody regulates everything (or at least in principle asserts the right to do so) or where a system of regulatory allocation is entirely predicated of might over right (i.e., enforcement jurisdiction), its practical or principled utility and efficacy is under threat. Where France does not just regulate France but also the rest of the world and where this principle is extended to every other State, the State-based system of law and order has broken down and lost its *raison d'être*. From a more close-up, constructive perspective, the routine non-applicability or displacement of the presumption in transnational internet cases requires its re-thinking and a re-framing. Such re-thinking would aim to reintroduce a measure of restraint and caution into competence assertions, so much so that not *every* foreign online provider who has contacts with local residents is *always* exposed to local law. The alternative is the demise of the Internet as a global communication space.

Thank you.

Min Jiang, UNC Charlotte

Graft Borders onto the Internet: Chinese Internet Sovereignty

Graft Borders onto the Internet: Chinese Internet Sovereignty

Min Jiang (Ph.D.)

Associate Professor @ UNC Charlotte
Secretariat Member, Chinese Internet Research Conference

The Internet in China Whitepaper

- "Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty… Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security."

  - State Council Information Office (2010)

"Computer education must start with kids"

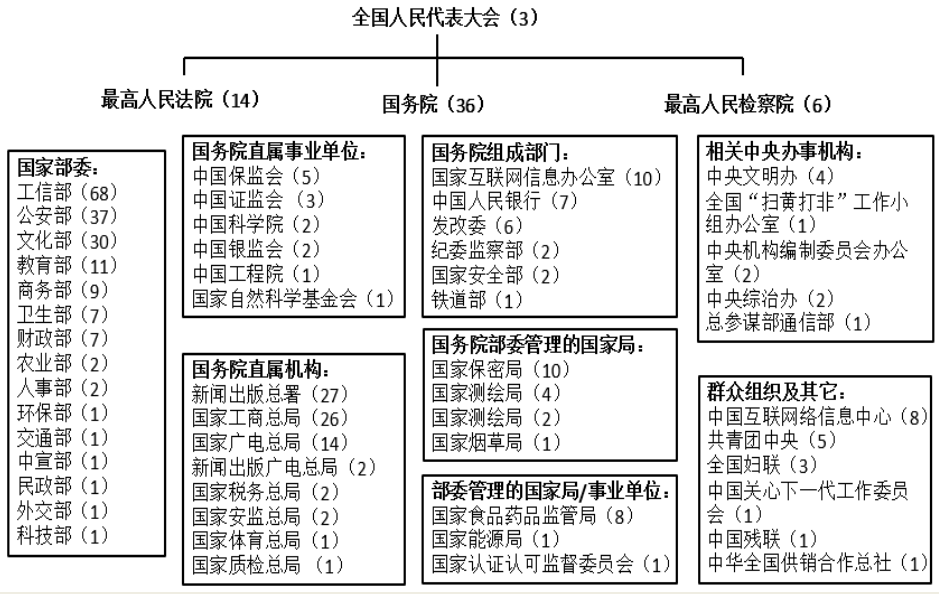
- Deng Xiaoping (1984)

"By linking with the Internet, we don't mean absolute freedom of information… If you go through customs, you have to show your passport. It's the same with management of information. There is no contradiction at all between the development of telecommunications infrastructure and the exercise of state sovereignty."

- Wu Jichuan (1995)

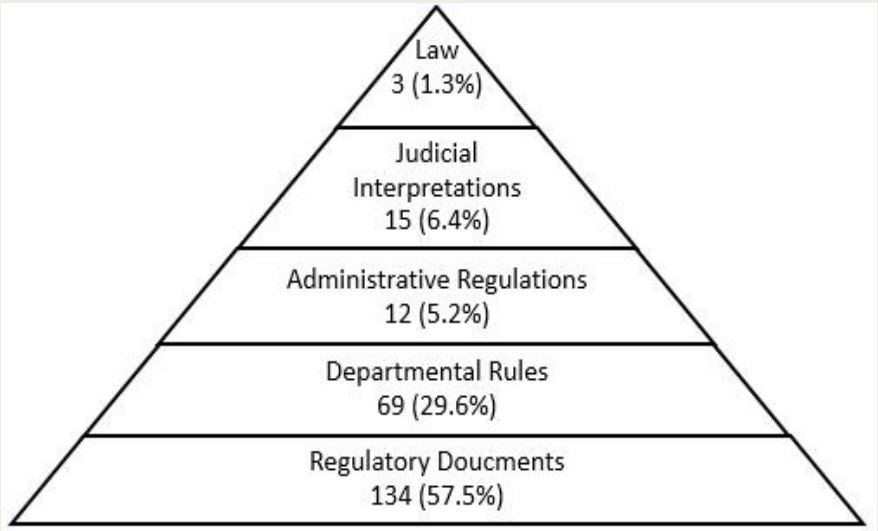
Former Minister of Posts and Telecommunications

Chinese Internet Regulatory Agencies



Source: Miao, Pang & Jiang (2017). Manuscript under review.

Regulatory Policies by Type
(1994-2015)



Source: Miao, Pang & Jiang (2017). Manuscript under review.

A New Internet World

- Re-nationalization of the Internet
  - *Return of borders, cybersecurity*
- No longer dominated by liberal values/practices
  - *22% "Partly Free" (Freedom House)*
  - *30% "Not Free"*
- Erosion of civil liberties in "democracies"
  - *NSA, Snowden Affair, Gawker, Trump*
- Global surveillance and filtering as the norm
  - *By states and Internet giants*

2-Trillion-Dollar Photo (2015)