Extraterritorial Enforcement:
Developing Norms for the Information Society

Workshop White Paper

December 2018

Hosted by
The Information Society Project
The Floyd Abrams Institute for Freedom of Expression

Funded by
Oscar M. Ruebhausen Fund (OMR)

Conference Co-Conveners
Sandra Baron, Resident Fellow, Information Society Project
Asaf Lubin, Visiting Fellow, Information Society Project

Student Reporters
Mailyn Fidler, Shlomo Klapper, Brian Mund, Will Horvath

Table of Contents

Introduction 3

Opening Panel: Clashing Visions for Control over the Internet 5

Roundtable I: Jurisdiction, Extraterritoriality, and Data Exceptionalism 9

Roundtable II: Data Conflicts and Future Regulation 13

Routes to Solutions 15

Appendix A: Workshop List of Participants 23

Appendix B: Workshop Agenda 24

Appendix C: Suggested Readings 27

Introduction

Recent years have seen a significant number of cases centered on conflicting jurisdictions and territorial over-reach in cyberspace.[1] Common to these litigations is a challenge to the power of states to control cross-border data transfers and offshore stored content and its distribution either directly, or indirectly, through internet intermediaries. The rise of social media platforms and online service providers, and their development and deployment of cloud computing, virtual server hosting, and anonymized and encrypted communication software pose the most recent disruptive assault on the power and legitimacy of sovereigns to assert their legislative control and adjudicative and enforcement jurisdiction.

On Friday, March 9, 2018, the Information Society Project (ISP) and the Floyd Abrams Institute for Freedom of Expression, with the generous support from the Oscar M. Ruebhausen Fund, hosted a workshop intended to explore the ongoing challenges to define these conflicts and discuss the viability and desirability of possible solutions. The concept for the day-long event was to bring together academics, corporate actors, private sector attorneys, and civil society advocates across disciplines and fields to discuss the way forward for contemporary debates surrounding these issues. The workshop consisted of high-profile experts, ISP resident and visiting fellows, and Yale Law School student attendees.

The workshop consisted of an opening panel followed by two roundtable discussions. The opening panel was set as an introductory panel framing the conversation by introducing some of the key cases and acts of legislation across the United States, Canada, and the European Union. The conversation then shifted to discuss two controversial and interlinked premises surrounding the debates on conflicts and the information society.

First, that one of the primary reason for the failure to resolve the internet jurisdictional puzzle to date lies in the compartmentalization of the discourse. Internet intermediary liability scholars don't talk to mutual legal assistance scholars; intellectual property practitioners don't engage e-discovery practitioners, who in turn don't engage data protection practitioners; freedom of expression professionals interested in content blocking and de-indexing find few opportunities to bridge the gap with their access to user data by law enforcement counterparts. The result is a conversation conducted in isolation, each group of thinkers operating within their pre-defined silos.

Second, that this compartmentalized conversation is causing a conflation of first order rules with second order rules, to a point where one would not be able to think of jurisdictional solutions separate from the subject matter being addressed. The workshop attempted to begin sketching out a broader panacea for conflict-of-laws in the information society by bringing scholars from across different fields to focus solely on jurisdictional and choice of law tensions.

The day proceeded with two different roundtable discussions. The first, *Jurisdiction, Extraterritoriality, and Data Exceptionalism,* examined the notions of sovereignty and

[1] These include *U.S. v. Microsoft*, *Google Inc. v. Equustek Solutions*, *CNIL v. Google Inc.*, *Richter v. Google Inc.*, and *X v. Twitter*.

jurisdiction (to prescribe, to adjudicate, to enforce) and their application in our data-driven world. Particular focus was given to the issue of how internet structures and certain features of the information society, may be forcing a redefinition legal concepts and rules that form that substratum of our international legal order. We analyzed cases from both the "access to data" and "control over content" buckets. The second, *Data Conflicts and Future Regulation*, looked to existing conflict-of-laws literature and jurisprudence, namely as they relate to the issue of choice-of-law and recognition of judgments. Such standards as the presumption against extraterritoriality, sovereign deference, and the principles of comity and reasonableness were examined and discussed. Particular attention was given to the likelihood and the effectiveness of treaty formation and international rule making surrounding the adaptation of these standards to the internet age. Both roundtable discussions provided the opportunity for meaningful discussion among the participants and generated several ideas for future litigation and policy work.

This workshop was meant to be a first step towards encouraging interdisciplinary conversation and work on these issues. The workshop was held under Chatham House Rules. This report highlights some of the many points raised during the day-long discussion. It does not represent the views of the individual participants, their affiliated institutions, nor the sponsoring organizations. Nor is this report a transcript; many points raised by participants have been rearranged by subject matter for readability.

Opening Panel: Clashing Visions for Control over the Internet

This panel framed the conversation by discussing some of the developments in the Internet & Jurisdiction project (with a focus on data access cases) and cases and controversies in Canada and the European Union. In general, the participants highlighted – and lamented – that in the conceptual clash between a jurisdictional world governed by territoriality and an online world that aims to transcend territory, courts and countries have universally hewed towards the former, territorial approach. They have espoused views, rulings, and internet-wide injunctions that, on the whole, have led, and will likely continue to lead to, the balkanization of the internet.

The first speaker introduced the work done the week before the Workshop at the Internet & Jurisdiction Policy Network within the Data & Jurisdiction and Content & Jurisdiction workstreams. The Roadmap described the goal: "All actors face a similar challenge: developing policy standards respecting privacy and due process that define conditions under which authorized law enforcement authorities can request from foreign entities access to stored user data necessary for lawful objectives." Further, the Roadmap outlined an extensive and useful list of issues that arise for data conflicts of law in three areas: data access, content takedown, and domain name system.

The second speaker spoke about the Canadian landscape. The speaker noted that Canada is a mix of the North American inclination towards media freedom and the European inclination towards privacy. The speaker then outlined two important, recent Canadian cases: *Google Inc. v. Equustek Solutions, Inc.* and *British Columbia (Attorney General) v. Brecknell*. *Google Inc. v. Equustek* began with a civil dispute heard at the court in British Columbia, Canada between Equustek Solutions and Datalink Technologies. Equustek, which markets technological products in British Columbia, claimed that Datalink had marketed its products in violation of Equustek's trademark and commercial secrets. During the legal proceeding, Datalink left Canada but continued to market its products via the internet.

The court found in favor of Equustek, establishing that Datalink had violated the company's intellectual property. It ordered Datalink to discontinue its operations. On the basis of this ruling, Equustek contacted Google several times and asked the company to prevent the indexing of Datalink's websites from Google's search engine. Google obeyed the judicial ruling by removing some 350 websites from the results page of its search engine, but it did so only from its Canadian site (Google.ca). Accordingly, users of all Google's other search engines, such as Google.com or Google.co.il, could continue to view Datalink's websites, which continued its violations. In the procedural instance and the appeal instance, the B.C. court twice ordered Google to remove the offending search results from all the search engines it operates around the world. Google appealed against this outcome, and the case eventually came before the Canadian Supreme Court. The Canadian Supreme Court rejected Google's appeal by a majority of seven justices to two, ruling that the company must remove search results leading to Datalink's websites from all its search engines. Regarding the international application of the order, the Supreme Court ruled that since the internet has no borders, the order must be applied wherever Google is active, in order to ensure its efficiency. To apply the order solely to Google.ca would be inefficient, since it enables Datalink to continue to sell its products (in Canada and elsewhere) to customers using Google's other search engines. The court rejected Google's argument that the international

application of the order violates the principle of comity in international law and forces Google to violate laws and protected rights under the legal systems of other states. It found that this was a theoretical argument that had not been properly proved. The court also discussed the balance of convenience between the two sides, and found that while Equustek's intellectual property was being violated repeatedly, Google would not incur substantial expenses due to the international application of the order. The speaker noted that the *Equustek* decision was disappointing in that it skirted around some of the thornier issues of the legality of global injunctions.

The minority opinion in the case found that that the order should not be applied internationally, for various reasons: The fact that Google is not a party to the proceeding between the two companies; the fact that the order granted requires close judicial supervision, since it must be updated from time to time as Datalink begins to operate at different web addresses; the determination that the order is inefficient, since Datalink's websites can be found by the general public by means of other search engines, by entering the relevant link to the company's website directly into their browser, by copying the link to the company's website by email, or through social media; and the fact that Equustek has access to alternative reliefs, such as the pursuit of proceedings in another territory in which it suspects that Datalink is active.

Google did not accept the ruling of the Canadian Supreme Court. On July 24, 2017, it asked the court in the Northern District of California to determine that the Canadian ruling should not be enforced. Google argued that the Canadian order also has ramifications for other content Google exposes as an American company to its American users. Global Google's argument against the order approved by the Canadian Supreme Court rested on three pillars: Firstly, the Canadian ruling violated the First Amendment to the U.S. Constitution, which protects freedom of expression, since the search results the company presents are protected under freedom of expression. Secondly, Section 230 of the U.S. Communications Decency Act (CDA) establishes that a service provider will not be considered to be "publishing" content created by a third party, while the Canadian order de facto regarded Google as the publisher of the violating content. Thirdly, the Canadian order violates international principles requiring states to refrain from interfering in the domestic affairs of another state and to refrain from issuing orders that apply in the territory of another state.

On November 2, 2017, the Californian court accepted Google's application and issued a temporary declarative order stating that the ruling of the Canadian Supreme Court is not to be enforced within the borders of the United States.[2] The Court noted that Google demonstrated it is entitled to immunity for Datalink's speech under Section 230 and that the U.S. Congress in enacting Section 230 sought to make free speech on the internet "unfettered and unregulated," preserving a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity. The Canadian court order, therefore, from the perspective of the U.S. court, "undermines the policy goals of Section 230 and threatens free speech on the global internet."[3]

[2] The temporary finding became a final ruling on December 14, 2017.

[3] For criticism of the decision, see Barry Sookman, *US Court Thumbs Its Nose at Supreme Court of Canada: Google v Equustek* (Feb. 18, 2018), http://www.barrysookman.com/2018/02/18/us-court-thumbs-its-nose-at-supreme-court-of-canada-google-v-equustek/.

Most recently, on April 16, 2018 in *Equustek Solutions Inc. v Jack*, the B.C. court responded to Google's request to reconsider its finding, in light of the U.S. court decision. The B.C. court rejected Google's requests. The B.C. court said that the U.S. decision (which was in Google's favor) did not establish that the injunction requires Google to violate American law. And without any significant change in circumstances, the court reasoned, there was no reason to change the original order. As a result, the temporary order against Google – which has been in place since 2014 – remains in place, pending outcome of the trial.

In *B.C. Attorney General v. Brecknell*, police were granted access to records and information relating to a posting on Craigslist. The Craigslist posting was said to be connected to a criminal offence alleged to have been committed in a B.C. community. Two lower courts refused to issue the production order (sought under a provision in Canada's Criminal Code) on varying grounds, including that Craigslist is a U.S. company with only a virtual presence in British Columbia. The Court of Appeal took a different approach, subjecting Craigslist to Canadian law. The court found there was a "real and substantial connection between craigslist and British Columbia arising from Craigslist's virtual presence in British Columbia to conduct business," sufficient to provide a jurisdictional foundation for the issuance of a production order. In recognizing the "realities of modern day electronic commerce," the court stated that Craigslist's virtual presence is closely connected to the circumstances of the alleged offense, because "at least some elements of the alleged offense were facilitated by relying on the services Craigslist provides virtually." The court concluded its reasoning with its viewpoint on the intersection of law enforcement and modern commerce: "In the Internet era it is formalistic and artificial to draw a distinction between physical and virtual presence . . . [Nothing turns on] whether the corporate person in the jurisdiction has a physical or only a virtual presence. To draw on and rely on such a distinction would defeat the purpose of the legislation and ignore the realities of modern day electronic commerce."

The speaker noted the broad reading of jurisdiction in Canadian courts. Like *Equustek*, *Brecknell* shows that Canada's courts will apply their jurisdiction more broadly in the internet era. A company no longer needs to be physically based in Canada to be subject to Canada's court procedures. The speaker also noted that the court did not consider important extraterritorial enforcement issues. Last, the speaker noted that while the Canadian courts claim to be proud of their judicial restraint and respect for comity, in practice, as these cases show, the truth is quite the opposite.

The last speaker spoke about trends in the European Union, highlighting three areas: data protection, cross-border access, and content control. As to data protection, the General Data Protection Regulation (GDPR), which came effect in May, gives the European Union full extraterritorial jurisdiction to any operator monitored by the GDPR. However, it does not deal with enforcement, except for goods enforcement, for which there is a requirement of the representative being physically present in the European Union. The e-privacy directive is claimed as a victory for strict privacy, holding service providers (rather than communication providers) to much stricter privacy requirements. The jurisdiction is essentially global – it does not matter where the interaction took place – and payment is not needed. For example, Skype, which is free, is still covered by this provision. In Joined Cases C-203/15 and C-698/15, the Court of Justice of the European Union (CJEU) disqualified UK-Swedish legislation regarding

data retention by telecommunications companies since there were inadequate safeguards governing access to communications data.

With relation to cross-border data access, the speaker discussed a few cases surrounding Europe. The speaker started with the two *Schrems* cases. *Schrems I* concerned a complaint aimed at prohibiting Facebook from further transfer of data from Ireland to the United States, given the alleged involvement of Facebook USA in the PRISM mass surveillance program. Schrems based his complaint on E.U. data protection law, which does not allow data transfers to non-E.U. countries, unless the company can guarantee "adequate protection." *Schrems I* resulted with the invalidation of the Safe Harbor regime between the United States and the European Union. *Schrems II*, now pending before CJEU, regards the utilization of standard contractual clauses as an alternative for continued data transfers. The CJEU has since struck down an E.U.-Canadian agreement regarding passenger names records (PNR) on July 26, 2017. The court found in Opinion 1/15 that "the PNR agreement may not be concluded in its current form because several of its provisions are incompatible with the fundamental rights recognised by the EU."

The speaker noted that the issues to watch are the U.K.-U.S. MLAT, which is now likely to be adopted as an executive agreement under the CLOUD Act.[4] The speaker further noted that there has been a backlash to the CLOUD Act in the form of leaked legislation by the European Union, the e-Evidence Initiative, discussed further below.

The last issue raised was content control. The speaker emphasized the importance of the French data protection authority (CNIL), which stated that there is no limiting principle on the Right to be Forgotten. The speaker emphasized that it is unusual how this became a universal right. It had been only four years since *Google Spain*, when E.U. Advocate General Niilo Jääskinen stated that the Right to be Forgotten, "would entail sacrificing pivotal rights such as freedom of expression and information," as individuals could seek to suppress "legitimate and legal information that has entered the public sphere." The speaker suggested that France breaches U.S. constitutional rights by requiring global delisting. Next, the speaker noted that the four major internet intermediaries (Facebook, Microsoft, Twitter, and Youtube) negotiated with the European Union about a Code of Conduct on Countering Illegal Hate Speech Online. The speaker noted that according to the European Commission reporting, IT companies "removed an average of 70% of illegal hate speech notified to them by the NGOs and public bodies." On the other hand, transparency and feedback to users is an area where further improvements should be made.

[4] For further reading about recent developments, see Peter Swire & Justin Hemmings, *Recommendations for the Potential U.S.-U.K. Executive Agreement Under the Cloud Act*, LAWFARE (Sept. 13, 2018), https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act.

Roundtable I: Jurisdiction, Extraterritoriality, and Data Exceptionalism

This session examined the different considerations in determinations of choice of jurisdiction and choice of law for the world of data. The discussion focused on four discrete areas of data challenges: choice of jurisdiction, choice of law, and the CLOUD Act, and choice of remedy.

Choice of Jurisdiction: Does Data Location Matter?

Participants questioned whether data location matters for data regulation. Some suggested that an emphasis on the location where data is stored reflected antiquated "dirt-clod" like thinking,[5] explained only because of the tendency to gravitate towards bright line simple rules. Others pointed out that normatively speaking, countries like China view data control as a means of furthering legitimate state aims over their territory. Descriptively speaking, because countries align to the territoriality of data, companies also consider data through a territorial lens. Some academics suggested governments should be given "front-door" access to data as a means of respecting legitimate state interests and preventing data localization and undesirable consequences to criminal investigations of withholding data access. Others, particularly privacy activists, suggested that such a decision was intolerable from a human rights perspective. Participants generally agreed that the current trend was a world headed towards data localization.

The participants also considered how jurisdictional thinking relates to access to markets and trade. For example, Latin America has a history of adopting data protection laws to promote transnational trade, and the United States has given extraterritorial effect to its antitrust laws.

Choice of Law: Who Should Choose?

Participants also debated whether an individual should be able to select the laws that govern their data, even in a data-localized world. Some advocated this idea as a rights-protective measure, while others saw this as fundamentally at odds with the rights and responsibilities associated with living in a particular territory. However, those against data choice of law suggested that there should be a baseline of human rights protection.

The CLOUD Act: A Step Forward?

In 2013, the inadequacy of the status quo in dealing with cross-border data access became starkly apparent when Microsoft refused to comply with a warrant issued under the 1986 Stored Communications Act (SCA) to hand over customer data stored in Ireland on the grounds that it did not apply extraterritorially. This *Microsoft Ireland* case went to the U.S. Supreme Court, where, prior to a decision on the substantive issues raised by the appeal, it was rendered moot after the U.S. Congress took action on the issue, tucking the Clarifying Lawful Overseas Use of Data (CLOUD) Act into the 2232 page 2018 omnibus spending bill. The CLOUD Act removed

[5] As one participant noted, personal property has always transferred by giving possession of the thing itself. In feudal land transfers, the seller presented a clod of dirt from the land to the buyer in the presence of witnesses to symbolize delivery of title. Today, the delivery of the deed constitutes the actual transfer of title to the land. Focusing on the location where the data is stored seems to be adopting a "dirt clod" way of thinking about control over data.

any sort of ambiguity — service providers could be compelled by warrant to disclose data, regardless of the location of that data. Only when the government seeks data of a foreigner living outside of the states and the request creates a conflict with the laws of a "qualifying" foreign government can the request be nullified on comity grounds. "Qualifying" foreign governments are those which have entered into executive data-sharing agreements with the United States and thus meet certain privacy and legal standards. It is vital to note that as of this writing there have been no executive agreements signed under the CLOUD Act, although the United States and the United Kingdom have been negotiating what could become the first executive agreement.

The discussants had diverging views relating to the Act. Privacy activists noted that it was a step forward but wished it were more privacy protective. In particular, they mentioned concern over the unilateral determination by the Attorney General and Secretary of State with regards to the adoption of new executive agreements.[6] Also, the CLOUD Act's balance of interest seems one that will give the United States access all of the time and thus will not necessarily solve the conflicts problem.

The participants also considered substantively what the correct privacy protections were. Some discussants took a sovereign deference approach, suggesting that the right protections are those in the country's laws. Privacy advocates wanted a high bar for protection standards, but recognized that such a standard would be self-defeating if the standards were so high that most countries could not get in – and therefore would not be regulated at all.

The passage of the CLOUD Act was supported by major U.S. technology firms such as Microsoft and Apple, as they felt it both offered adequate privacy protections and reduced the frequency of conflicts of laws, which could be economically ruinous. On the other hand, the somewhat unilateral approach taken by the United States drew the ire of privacy advocates and certain foreign governments. Johannes Casper, Hamburg's Commissioner for Data Protection, had argued that the CLOUD Act "is a law at the expense of privacy and the fundamental right to data protection, with potentially global proportions." Just what effect the CLOUD Act will have on international cooperation on this issue of cross-border data access is heavily dependent on the number of nations that will enter into executive data-sharing agreements with the United States as "qualifying" foreign governments. These "qualifying" foreign governments will be able to bypass the burdensome MLAT process to gain access to content stored in the U.S. provided that their requests meet certain standards, including that the request does not target U.S. citizens and that it "shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order." This language appears to open up the potential for requests without sufficient ex-ante judicial authorization, a key principle of human rights law. Nonetheless, Brad Smith, Chief Legal Officer at Microsoft, has called upon the United States to enter into executive agreements. He argued that "the CLOUD

[6] In accordance with the CLOUD Act, an executive agreement governing access by a foreign government to data shall be considered to satisfy the requirements of the Act "if the Attorney General, with the concurrence of the Secretary of State, determines, and submits a written certification of such determination to Congress." The requirements include that that the foreign government "demonstrates respect for the rule of law and principles of non-discrimination," and that it "adheres to applicable international human rights obligations and commitments," including rights to privacy, due process, fair trial, freedom of expression, and prohibitions against torture and cruel, inhuman, or degrading treatment.

Act's approach to international agreements helps point towards the modernization of international law the world needs."

As was mentioned above, in response to the CLOUD Act, the European Commission proposed similar legislation, unveiling the e-Evidence Initiative on April 17, 2018. Just like the U.S. law, the proposal would allow law enforcement to obtain data directly from a provider regardless of where that provider is located. The e-Evidence Initiative does this through two complementary components: a proposed regulation and directive. The regulation would provide for European Production and Preservation orders that would allow a judicial authority in one member state to compel a service provider in another member state to produce or preserve stored data. The directive would require any provider offering services in the European Union to designate a legal representative that "shall reside or be established in one of the Member States where the service provider offers the services." This would ensure "that all providers that offer services in the Union are subject to the same obligations, even if their headquarters are in a third country." In this way member states in the European Union would be able to unilaterally access data subject to certain safeguards, including "the principles of necessity and proportionality, due process, data protection, secrecy of correspondence and privacy."

Article 15 of the Directive sets out procedures for when the provider believes compliance with a request would lead to a conflict of laws. It is significant to note that unlike the CLOUD Act, if a conflict would violate a law in the state where the order is executed regarding "the fundamental rights of the individuals concerned" or "the fundamental interests of the third country related to national security or defence" the issuing state would have to notify the second state, and that state would have the opportunity to lift the order if it objected. In this way the e-Evidence Initiative offers less unilateral access to data than the CLOUD Act, and arguably would facilitate greater cooperation.

Many in the European Union have been hoping to pass the e-Evidence Initiative by December 2018, but there have been many roadblocks, including controversy over whether a member state that issues a European Production Order (EPO) should have an obligation to notify the member state in which the provider resides and of which the target is a national, potentially giving those states the opportunity to quash the EPO.[7] It is important to note that the e-Evidence proposal is still evolving, with a goal of finishing by December 2018. Theodore Christakis describes the challenges posed by the notification problem as similar to "the myth of the Lernaean Hydra: for every head chopped off, the Hydra would regrow two heads and for every question answered in this article, two new queries might emerge."[8]

[7] Theodore Christakis, *"Big Divergence of Opinions" on E-Evidence in the EU Council: A Proposal in Order to Disentangle the Notification Knot*, CROSS-BORDER DATA FORUM (Oct. 22, 2018), https://www.crossborderdataforum.org/big-divergence-of-opinions-on-e-evidence-in-the-eu-council-a-proposal-in-order-to-disentangle-the-notification-knot/.

[8] *Id.*

Choice of Remedy: How To Resolve?

The session also addressed extraterritorial content challenges. The participants struggled to extract general principles governing these challenges, and instead they noted that courts engage in a balancing test that does not focus on the location of data servers. Particularly, courts decide based on whether there was harm in their country and if courts have power to construct an available remedy. Some participants suggested that a better jurisdictional analysis would inquire into whether the defendant was "purposefully availing" themselves of the jurisdiction. Currently, courts scope a remedy based on the actors in their jurisdiction, regardless of whether they were in fact bad actors. Google may not be guilty of anything more than serving as a vehicle for an illegal actor to pursue his bad acts, but Google is the one from which the remedial action crafted by the adjudicating body is sought and enforced. This threatens the interests of current and potential multinational corporations.

However, the alternative leads to an *Equustek* scenario in which a successful party may face the need to file thousands of takedown requests and separately in each jurisdiction in order to gain the benefits of an effective remedy. Some questioned why the sheer number should make a difference in the analysis. Others pushed for a flipped presumption so that the person who wants the content removed should bear the burden of proof.

The participants considered a number of cases, including *Die Grünen v. Facebook Ireland Limited*. The Austrian Court of Appeal ruled in May 2017 that Facebook must delete all hate postings and verbatim re-postings against Austria's Green party leader, Eva Glawischnig, not just in Austria but worldwide. The case was brought by Austria's Green party after Glawischnig was insulted on Facebook by posts from an internet troll. The Court said that an individual's right to protection of dignity and reputation had to be balanced against the European Convention on Human Rights (ECHR) Article 10 right to freedom of expression, including political expression. However, it reasoned that the postings, which referred to the Austrian Green Party Leader as a "corrupt tramp" and "lousy traitor," went beyond political comment and were clearly aimed at insulting and vilifying Glawischnig personally. They were thus not legitimate criticisms and therefore could not be protected under Article 10 of the Convention. The Austrian Supreme Court referred the case to the CJEU to consider the adequacy of extraterritorial global injunctions.

Participants generally agreed that hate speech poses different challenges than data protection writ large. One problem identified in the content removal cases surrounds the practical challenge of whether one can realistically ask a company to not only monitor for certain terms but also for certain sentiments. Some suggested that this problem is particularly troublesome given the E.U. movement to hold companies accountable rather than the individual plaintiffs. The panel concluded by recognizing the persistence of a conflict between the people wanting more substantive speech protection and those who want greater data protection.

Roundtable II: Data Conflicts and Future Regulation

This session focused on possibilities for resolving data conflicts in the long-term future. The discussion centered around two main questions: Who are the right actors and institutions to resolve these conflicts? Does approaching data conflicts topic-by-topic or as a whole best suit resolving these conflicts?

Courts have been at the forefront of data jurisdiction conflicts. Despite their active role, however, courts are necessarily limited in their approach to problems. Courts have limited capacity to handle the volume of cases in the data jurisdiction space, facing a task of setting precedent in a fast-paced, quickly evolving environment. Courts also have a clear mandate to protect their own citizens. The repeat fact pattern in data jurisdiction cases – often a large, foreign corporation harming an individual – incentivizes courts to find in favor of the harmed individual in their own jurisdiction. Additionally, fact patterns involving a smaller private entity and an individual claiming harm may not make it to court, further skewing court outcomes. For every litigation, many disputes are resolved outside of courts. Overall, the courts' institutional mandate and limited view of cases can prevent it from adequately weighing larger, overarching considerations, especially those between nations.

Data jurisdiction conflicts between the European Union and the United States can be seen as conflicts between deeply held views about fundamental rights to speech and privacy. This deeply cultural and political topic may be better resolved outside the courts through institutions better able to take such considerations into account. Clashes of fundamental rights have historically been hard to solve, within and between nations. Participants discussed possible additions or alternatives to the courts as primary institutional actor on data jurisdictional questions.

International negotiations are one alternative, ranging from multilateral to bilateral agreements between countries on data matters, such as the recently introduced U.S. CLOUD Act. International negotiations can take into account broader perspectives than party-based litigation. Still, these negotiations could lack the transparency needed to make sure these agreements adequately protect data holders' interests and both countries' interests.

In what is effectively the opposite solution, countries could agree that each state gets to do what it wants within its borders. This option was not particularly popular among participants, given its implications for global interaction. Still, national governments are an important institutional player to recognize.

If courts remain the central institutional actors, a more rigorous conflicts of law approach could help resolve some data jurisdiction conflicts. Returning to traditional conflicts of law analysis such as choice of jurisdiction, choice of law, and choice of remedy could bring more predictability to data conflict jurisprudence. A shared legal analysis adopted by the courts would help integrate domestic legislation, bilateral agreements, and multilateral agreements into a more standard jurisprudence.

Last, private actor solutions offer another avenue. With previous internet jurisdictional debates, including over e-commerce, private actors found workable solutions, especially through

contractual solutions, such as terms of service, and technology solutions, such as geoblocking. Private actors seem more hesitant to spearhead resolution of data jurisdictional questions – perhaps because the political stakes are higher. Stuck between a rock and a hard place, tech companies carefully tread waters, to ensure their business continuity across these different regions and countries.

Routes to Solutions

Framing the Debate: Defining the Scope of Data Conflicts

The rise of social media platforms and online service providers, and their development and deployment of cloud computing, virtual server hosting, and anonymized and encrypted communication, are forcing national courts seeking to address the internet's local effects on plaintiffs coming before them to engage in increasing volumes of extraterritorial adjudication through the issuance of interstate and global orders. This creates jurisdictional tensions which result in challenges to the power of Courts and Legislatures to control cross-border data transfers and offshored stored content either directly, or indirectly through internet intermediaries.

Consider the following cases, some of which were discussed at greater length above:

1. *U.S. v. Microsoft.* FBI seeks access to emails pertaining to a drug-trafficking case stored on a server in Ireland. Case might be moot with passing of the CLOUD Act.
2. *Google v. Equustek Solutions.* Global de-indexing of Google search results for an IP-violating company.
3. *Google v. CNIL.* French data protection authority demands from Google to delist articles from its search results on Google Domains worldwide on RTBF grounds.
4. *LICRA v. Yahoo.* French League Against Anti-Semitism seeks removal from Yahoo's online auction services the sale of Nazi memorabilia.
5. *Belgium v. Skype.* Belgian Court order compelling Skype to disclose both content and non-content pertaining to a crime committed on Belgian soil. Skype claimed to be registered in Luxembourg and thus Belgian courts lacked jurisdiction. Claims were denied, based on a previous similar ruling in *Belgium v. Yahoo*.
6. *Beluga Shipping v. Suzlon Energy.* Australian Turbines company seeking access to U.S.-stored Gmail accounts of former employees, in discovery for a civil suit on fraud.
7. *Eva Glawischnig v. Facebook.* Seeking CJEU clarification as to whether Facebook has an obligation to globally remove "hate speech" from its platform (a post calling the former Austrian Green Party Leader a "corrupt tramp" and "lousy traitor").
8. *British Columbia (Attorney General) v. Brecknell.* Canadian Police seeks to unmask a Craigslist user for unspecified crimes allegedly committed in British Columbia. All data is stored on U.S. Servers and Craigslist had only "virtual presence" in Canada.
9. *Richter Morales v. Google.* A Mexican lawyer suing to remove a defamatory blog hosted on Google's Blogger.com platform accusing him of money laundering.
10. *X v. Twitter.* New South Wales Supreme Court compelling Twitter at the request of an Australian corporation to both unmask and remove all accounts of a twitter troll who falsely used the CEO's name to disclose confidential financial records relating to the company.
11. *Russia v. Google.* Russian regulator Roskomnadzor launched a new civil action against Google for failure to comply with a 2017 law forcing "social companies" to remove access to content deemed by Russia as illegal within twenty-four hours. Legislators debate increasing fines for up to 1% of annual revenue.

12. *Ben Hemo v. Facebook.* Israeli litigant brought a class action lawsuit against Facebook for violating the privacy rights of the class by storing the content of personal messages on the social platform and sharing them with third parties for profit. Facebook argued, in accordance with its terms of service, all cases are to be heard before California courts under California law. The Israeli High Court of Justice ruled that Facebook's choice-of-courts provision would deprive Israeli litigants of their right to access justice and deter them from bringing future suits to protect their interests. Facebook, by providing services and conducting its business in Israel, should thus be exposed to potential litigation in the Country. The court ruled that in all similar cases actions will be brought before Israeli Courts who will apply California law, unless that law will deprive Israelis of their constitutional rights.

It would be misleading, however, to only look at cases that reach the courts, as not all conflicts get litigated. When Apple decides to store Chinese iCloud accounts and encryption keys in China to comply with data localization laws, it introduces the potentiality of multiple conflict-of-laws issues. So is the case when Instagram complies with Russian Telecommunications Regulator's threats and globally removes allegedly defamatory content against a Russian businessman. The same is also true when Twitter and Facebook decide to voluntarily and proactively remove accounts engaging in "inauthentic coordinated activity" ahead of the U.S. midterm elections.

Ultimately all data conflicts can be put into the following grid:

A. Access to Data Cases

1. Law Enforcement Requests (Criminal/National Security)
    a. Access to User Data
    b. Decryption, Backdoors, and Other Forms of Compelled Assistance
    c. Unilateral Remote Direct Access *(e.g.* Hacking by Law Enforcement)
2. E-Discovery Cases (Civil)
    a. Unmasking Anonymous Users
    b. Compelled Disclosure of Social Media and Other Electronic Evidence
    c. Access to Data Stored on Private Devices
3. Data Protection Cases (Civil, Administrative)
    a. Data Breaches and Privacy Class Actions
    b. Privacy enforcement and Statutory Fines (*e.g.* GDPR)

B. Data Control Cases

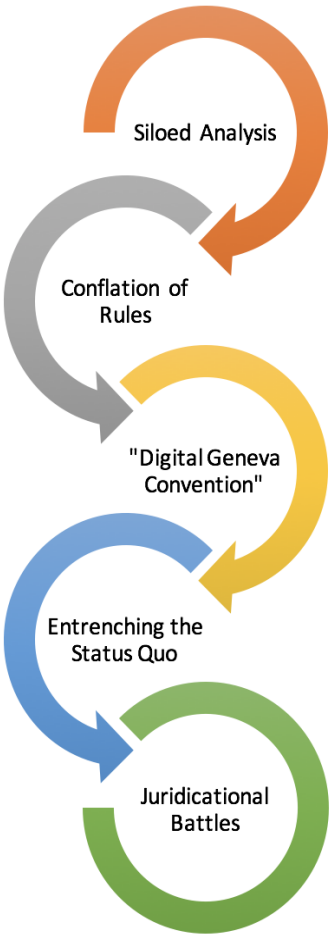
1. Content Takedown
2. Content Filtering
3. Content Blocking
4. Account Suspension
5. De-Indexing
6. Domain Suspension

Abusive Content: Hate speech, IP violations, RTBF, incitement to terrorism, "fake news", revenge porn, etc.

Infrastructure Abuse: phishing, malware distribution, botnet support, etc.

The Limits and Dangers of the Existing Discourse

This workshop was predicated on the assumption that part of the reason for the failure to resolve the jurisdictional puzzle to date lies in the compartmentalization of the discourse. Internet intermediary liability scholars don't talk to mutual legal assistance scholars; intellectual property practitioners don't engage e-discovery practitioners, who in turn don't engage data protection specialists; freedom of expression professionals interested in content blocking and de-indexing find few opportunities to bridge the gap with their access to user data by law enforcement counterparts. The result is a conversation conducted in isolation, with each group of thinkers operating within their pre-defined silos.



The main casualties of siloed conversations are procedural ideas. When conversations are sealed off from one another, first order rules are conflated with second order rules, to a point where one would not be able to think of jurisdictional solutions separate from the subject matter being addressed. We begin to think that we cannot solve the excess of jurisdiction issues at the heart of some of the above-discussed conflicts without first solving the MLAT problem or reaching a consensus around Section 230 immunities.

The first U.N. Special Rapporteur on the Right to Privacy, Joseph Cannataci, said that the "world needs a Geneva convention style law for the Internet to safeguard data and combat the threat of massive clandestine digital surveillance." Microsoft has adopted a similar position. This is a mistake.

The reality is that we don't need a Geneva Convention, we need a Hague Convention. Given that it is very unlikely that countries will be able to reach a consensus around what balances are needed for privacy and security, or for freedom of expression online, we should turn to private international law agreements (as opposed to public international law ones)[9] to provide some clarity and uniformity. **Though we might not agree on what to do, we might agree on what to do when we don't agree what to do**.

Lacking substantive proposals for solving the internet jurisdictional puzzle, lip service is paid in courts to conflict of laws principles. Litigants are reluctant to antagonize judges with complex conflict-of-laws analyses, preferring fast solutions with lesser chances of complicated sticky

[9] Given that many of the substantive issues revolve around fundamental value conflicts – between, for instance, freedom of expression and the right to be forgotten – they are unlikely to be resolved in a global fashion. In order to get a broad number of states to agree to an international treaty on substantive data matters, that agreement will necessarily be based on a lowest common denominator, which would represent a significant threat to due process given the undemocratic state actors who would need to be involved in order for such a treaty to have bite. Alternatively, if the agreement begins with a small club of like-minded states with robust due process protections, it will be small and therefore ineffective. Further, it would have skirted around the hardest conflicts cases, which involve states with questionable motives or fewer due process protections.

precedents. In turn, judges react with a shrug and a smile to such doctrines as "comity", "sovereign deference" and "presumption against extraterritoriality." The results are "Internet-Wide Injunctions," "Blocking Provisions," and "Data Localization" laws, all being issued as part of a broader battle over competing visions for internet governance. Goldsmith and Wu's prediction of a "technological cold war" has never felt so close.[10] In the midst of it we might see the balkanization of our connected life.

Below we discuss proposals for what a **comprehensive conflict of laws approach for the information society** might look like. Some of the elements were discussed throughout the workshop, though none of these have been endorsed by all participants and they should not be understood as conclusive. Rather, we hope that these ideas could help spur further conversation **towards a potential "Hague Convention on Jurisdiction, Applicable Law, Recognition and Enforcement in Respect of Data Access and Data Control."**

By rejecting, for the time being, the lofty goal of a "digital Geneva convention" and proposing a more modest conflict-of-laws approach for regulation, we embrace what Andrew Woods calls a "sovereign-difference ideal" for internet governance. As he explains it:

> If the early debates about internet governance were about whether states had the power to regulate internet conduct, today's debates (as we have seen) are about which states' rules should apply and where. There are, generally speaking, two competing visions of internet governance today: (1) a cosmopolitan ideal that aspires to one set of rules everywhere, which is diametrically opposed to (2) a sovereign-difference ideal that sees the internet operating differently in different places according to local norms, customs, and rules... The most compelling defense of sovereign deference in cross-border data disputes is that it offers the best chance at creating the kinds of norms needed for a lasting and global internet. Sovereign states retain the capacity to regulate and control the internet, and they are going to exercise that control differently . . . .[11]

However, where Woods only proposes more general, and at times quite amorphous, doctrines such as "comity," we might benefit from seeking to develop a more robust framework that systematically applies the full corpus of conflict-of-laws to these cases. Such a framework will consider doctrinally each section of a conflict-of-laws analysis from choice of jurisdiction, to choice of law, to choice of remedy, to choice of enforcement. The goal could be to lay down the foundation for a potential Hague Convention, that could be developed by the Hague Conference on Private International Law (HCCH). The HCCH, which first convened in 1893, is an intergovernmental organization that develops and administers several private international law conventions. Its membership is comprised of 82 Member States as well as the European Union.

Within the limits of this white paper we cannot articulate all elements that could go into such a treaty, but we will highlight a few high-level ideas for consideration and further discussion.

[10] JACK GOLDSMITH AND TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 238 (2006).
[11] Andrew Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328, 366-367, 371 (2018).

1. **Choice of Jurisdiction**

   a. The traditional doctrines have been predominately territorial (*see, e.g.*, the Harvard Draft Convention on Jurisdiction). However, focusing only on the nationality of the intermediary, the Data Subject, or the harmed individual, or on their locus of control and action, seems arbitrary. As we saw with the Second Circuit decision in the *Microsoft Ireland* case, making choice of jurisdiction decisions based on the territory where the data just happens to be stored makes little sense as an organizing principle in the cloud computing age, given that data is divisible, location independent, intermingled, and constantly on the move.

   b. The current state of play, however, is equally troublesome. Courts bend over backwards to find their jurisdiction, basing their reasoning on the flimsiest of connections. Most cases apply an "active participation in economic life" or "offering services" test to deem corporations subject to the personal jurisdiction of courts. Others find their jurisdictional hook in the "effects test" looking at whether effects of the measure are felt or would be felt in the forum states.

   c. The landmark *International Shoe Co. v. Washington*, 326 U.S. 310 (1945), began a shift towards "long arm jurisdiction," which seeks to identify certain "minimum contacts" to establish jurisdiction. The problem we have been facing is the inability to articulate what should be those "minimum contacts" that would trigger the applicability of personal jurisdiction in the context of data conflicts.

   d. In an event hosted by the Stanford Center for Internet and Society in October 2016, participants were asked "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?" The kind of activities considered were: (i) Content is accessible in the forum state; (ii) Defendant has minimum contacts in the forum state; (iii) Defendant targets or directs actions to the forum state; (iv) Defendant makes money from the forum state, (v) Content is stored in the servers in the forum state; (vi) Defendant's locus of control or action is in the forum state; and (vii) Harm is in the forum state. The Stanford participants could not agree which of these were sufficient to establish jurisdiction and generally tended to argue that all of them were "relevant but not sufficient."[12] This finding is telling and suggests that we might be able to conceive of a kind of a "balance of convenience" test to determine choice of jurisdiction. It seems that relying on any one of the links above discussed as the single test for allocation of *situs* to intangible property would be arbitrary. We therefore might instead benefit from weighing all of these links together, to determine the most closely connected forum, the "center of life" of a particular piece of data. This would be akin to adopting the terminology of the Israeli *HCJ Gonen v. Haifa Income Tax Officer*, 477/02 (2005), which was introduced for the purpose of determining jurisdiction in tax cases for individuals operating in multiple jurisdictions.

[12] Stanford Center for Internet and Society, *Law Borders and Speech: Proceedings and Materials* 48 (Daphne Keller ed., 2017).

Choice of Law

a. In a 1972 landmark decision,[13] the U.S. Supreme Court shifted focus towards party autonomy. The current state of affairs seems to favor "our laws and our way all the time." But as the Supreme Court highlighted, industries in a globalized world will be disadvantaged and stifled in their expansion and development if "we insist on a parochial concept that all disputes must be resolved under our laws and in our Courts." As the court claimed, "we cannot have trade and commerce in world markets and international waters exclusive on our terms, governed by our laws, and resolved in our courts." The court thus opened the door for parties to expressly choose which laws they want to govern them.

b. The same is true in the internet age. We can reimagine a data subjects' right to articulate their choice of law. Terms of service could thus be re-written to introduce the potential for data subjects to choose which law they wish to see applied to their data. That law could govern in lieu of either alternative bright line choice of law rules and in isolation from the forum selected to hear the dispute.

c. In certain cases, the data subjects' desires will be unknown. This could happen, for example, where the data subject did not directly receive services from the intermediary and therefore did not enter intro contractual relationship with the intermediary.[14] We might still be able to protect data subjects' autonomy, in those cases, by applying the *pro-personae* principle –applying the "most favorable law," one that will benefit the reasonable data subject. An alternative version of this could be to apply all relevant laws, and insisting that the access-to-data request or control-over-data request be approved under all of those laws prior to the granting of an affirmative order. In other words, it would suffice that at least in one country the law would reject the request for a court to refuse to grant the requested warrant or injunction.

d. In this regard, note the doctrine of dépeçage, which establishes that different issues within a case may be governed by the substantive laws of different countries. The concept originated in civil law countries, but has also been adopted in common law countries, including in the United States.[15] It offers an "Issue-by-Issue Analysis" for conflicts of laws in the information society, so that we can apply one set of laws for privacy protection and another set of laws for protection of freedom of expression in the same case.[16] Symeonide summarizes the benefits of applying dépeçage:

[13] *The Bremen v. Zapata Off-Shore Company*, 407 U.S. 1 (1972).

[14] For example, the *Google Gmail Privacy Lawsuit* was brought by people who never used Gmail but only emailed people who did and were thus caught in Google's dragnet. Similarly, this situation could be created when one uses Youtube or Google Search without first establishing an account.

[15] For a survey of application of dépeçage in U.S. Courts *see* Symeon C. Symeonide, *Issue-by-Issue Analysis and Dépeçage in Choice of Law: Cause and Effect*, 45 U. TOL. L. REV. 751 (2013).

[16] Note potential criticism to this proposal. DAVID F. CAVERS, THE CHOICE-OF-LAW PROCESS 38 (1965) ("True it is that choice of law must proceed on an issue-by-issue basis; but modern conflict-of-laws analysis can make no more serious mistake than to indulge in an **unprincipled eclecticism**, picking and choosing from among the available

> Sports analogies are rarely an elegant way to express legal dilemmas, but there is a certain similarity between a court's predicament regarding dépeçage to that of a quarterback in possession of the football. If he throws the ball, three things can happen, and two of them are unfavorable—incompletion and interception. If, for this reason, he never throws the ball, his team's chances of scoring will be very low. In undertaking an issue-by-issue analysis, a court faces much better odds. Indeed, the court risks virtually nothing, except perhaps a few hours of extra work, by undertaking an analysis that is more likely than the traditional wholesale analysis to yield more nuanced and individualized solutions to conflicts cases.[17]

e. Alternatively, we can simply follow the rules discussed above for choice of jurisdiction. In the same way we adopted a "center-of-life" center for determination of jurisdiction, we can continue that analysis for the determination of the applicable law. This was the position of the New York Court of Appeals in the seminal case of *Babcock v. Jackson*, 191 N.E.2d 279, 283 (N.Y. 1963),[18] where the Court ultimately found that the governing law should be the law of the state which, "because of its relationship or contact with the occurrence of the parties, ha[d] the greatest concern with the specific issue raised in the litigation."

2. **Choice of Remedies**

We can introduce myriad restraints on choice of remedies, which are rooted in an adoption of the "least intrusive means" test for achieving the aims sought. This is a structure that disfavors global injunctions and blocking statutes, and instead promotes domain limited remedies, location limited remedies (geo-Blocking), temporally limited remedies, volume limited remedies, and judicially-limited remedies (such as an injunction that applies everywhere, "except where doing so would conflict with domestic laws"). Woods notes that "even with the cross-border cloud, courts can fashion cross-border remedies that contain built-in restraints. They have wide latitude in fashioning these remedies, and they often will do so with an eye toward other sovereigns, or they will not but the remedy will nonetheless be limited unilaterally by that sovereign."[19] Consider this possibility in light of the back-and-forth between Canadian and U.S. courts in *Equustek*.

---

laws in order to reach a result that cannot be squared with the interests of any of the related states. **Issue-by-issue analysis should not result in the cumulation of negative policies to produce a result not contemplated by the law of either state**") (emphasis added). Citing to Brainerd Currie, Cavers cautions against the creation of "synthetic hybrids," ones which are "half a donkey and half a camel."

[17] *See* Symeonide, *supra* note 15, at 772.

[18] Babcock involved an intrastate tort, a single-car accident, which occurred in the Canadian province of Ontario, but in which both the defendant driver and his injured passenger, the plaintiff, were domiciled in New York. Ontario had a "guest statute," which would bar the passenger's action because of her status as a gratuitous guest in the defendant's car. The court refused to apply that statute and instead applied New York law, which allowed the action.

[19] *See* Woods, *supra* note 11, at 378.

3. **Choice of Enforcement**

There should be a presumptive finality and sovereign deference surrounding choice of enforcement. States might only be allowed to refuse to enforce a judgment in cases of excess of jurisdiction, serious departure from a fundamental rule of procedure, insufficient reasoning, or a risk to foundational public policies. The HCCH 2018 Draft Convention on the Recognition and Enforcement of Foreign Judgments offers a good launching pad. Note that the draft in its current form already applies to cases involving privacy, defamation, intellectual property and analogous matters, and law enforcement activities. The more states could reach a consensus around choice-of-jurisdiction, choice-of-law, and choice-of-remedy rules, the less likely that courts would face challenges to enforcement.

Appendix A: Workshop Participants

Sandra Baron, ISP

Geff Brown, Microsoft

Jonathan Cardenas, ISP

Patrick Carome, WilmerHale

Rebecca Crootof, ISP

Jennifer Daskal, American University

Mailyn Fidler, ISP

Corynne McSherry, Electronic Frontier Foundation

Thomas Kadri, ISP

Lanah Kammourieh Donnelly, Google

Daphne Keller, Stanford

Shlomo Klapper, ISP

Tiffany Li, ISP

Robert Litt, Morrison Forester

Asaf Lubin, ISP

Vivek Mohan, Apple

Brian Mund, ISP

Caroline Wilson Palow, Privacy International

David Price, Google

Jacob Rogers, Wikimedia

Paul Schabas, Blakes

Jessica Simor QC, Matrix Chambers

Appendix B: Workshop Agenda

Opening Panel: Clashing Visions for Control Over the Internet

This panel is set as an introductory panel, framing the conversation by introducing some of the key cases and acts of legislation across three jurisdictions: the United States, Canada, and the European Union. Central to the discussion would be the question of what visions of internet governance are reflected in the laws and practice of each of these jurisdictions.

Questions for potential discussion:

(1) To what extent do these "internet-wide injunctions" by national courts lead to a "race to the bottom" or a balkanization of the internet? What are the dangers from such balkanization? Could there be any benefits?
(2) What is the extent to which courts that issue global injunctions are also concerned with their foreign enforcement? What is the extent to which reciprocity plays a role in judicial enforcement of such global orders?
(3) Is the inability of the western world to put forward a uniform and coherent internet governance agenda causing the entrenchment of data localization and digital rights encroaching policies across the global south? How should we best address the opposite visions for the information society emerging from such countries as: China, Russia, and Brazil.
(4) Are courts the wrong forum in which to engage in this battle for control? What alternative forums could offer a more adequate venue in which to develop greater uniformity and consensus around these debates on jurisdiction and enforcement power?
(5) What is the role of corporations in this space? How has their role been reflected in each of the jurisdictions? Are they the custodians and gatekeepers of the information society, or rather placed in the chokehold of governments seeking to assert their jurisdictional control? How can corporations play a more effective role in advancing their own visions for internet governance? What is the promise and limits of those corporations' self-regulation and harmonization through global terms of service for their platforms?

Roundtable Discussion I: Jurisdiction, Extraterritoriality, and Data Exceptionalism

Examining the notions of sovereignty and jurisdiction (to prescribe, to adjudicate, to enforce), and their application in our data-driven world. Particular focus will be given to the issue of how internet structures and certain features of the information society, may be forcing the redefinition of legal concepts and rules that form that substratum of our international legal order.

Questions for potential discussion:

(1) How should we resolve the tension between a seemingly a-territorial global network and an intrinsically territorial legal order?
(2) Scholars have proposed different tests for determining jurisdiction in cyberspace over the past few years. Amongst those are the following standards. Which of these is most appealing? Are there additional proposals? Are these proposals impractical or

ineffective? What kind of jurisdictional tests could we devise that would not result in forum shopping for litigants?

a. The nationality of the corporate entity, their locus of control or action;
b. The nationality of the person whose data is being sought, their locus of control or action;
c. The location where the data is being accessed.
d. The location where the data is being stored;
e. Whether the data is "meant to be accessible" from the territory of the state claiming jurisdiction (Tallinn Manual 2.0);
f. The location of the prospective harms (harms likely to result from a failure to access, de-index, block, remove, or otherwise manipulate the data in question);
g. "Totality of the circumstances" evaluation, taking into consideration all of the other criteria so to establish the "center of life" for a particular piece of data.

(3) Does jurisdictional analysis even merit this discussion? Should we not accept as inevitable the concurrent and residual jurisdiction to legislate and to adjudicate of all jurisdictions in cyberspace?
(4) Will the continued evolution of cloud base storage, including virtual server hosting, result in even more complicated jurisdictional issues? Alternatively, is the way the market of internet infrastructure consolidating towards a few major hosting providers be the end to the cross-jurisdictional competition? Where is the technology going and how will that impact these conversations?
(5) Recalling the 90s scholarly debate between Johnson, Post and Goldsmith (*Law and Borders – The Rise of Law in Cyberspace, Against Cyberanarchy, Against Against Cyberanarchy*) and the contemporary debate between Daskal, Svantesson, and Woods (*The Un-Territoriality of Data, Against Data Exceptionalism, Against Against Data Exceptionalism*): Is cyberspace truly a new legal frontier and is data truly a subject for *sui generis* jurisdictional regulation?
(6) Why do corporations tend to avoid raising jurisdictional challenges in courts, or frame their challenges as conflict-of-law jurisdictional challenges?
(7) In what cases have geo-location and geo-blocking tools proved useful in resolving cross-border jurisdictional conflicts? Where have they failed? Why? How may advancements in the technology be able to help mitigate those failures?

Roundtable Discussion II: Data Conflicts and Future Regulation

The focus of this roundtable will be on existing conflict-of-laws literature and jurisprudence, namely as they relate to the issue of choice-of-law and recognition of judgments. Such standards as the presumption against extraterritoriality, and the principles of comity and reasonableness will be examined and discussed. Particular attention will be given to the likelihood and the effectiveness of treaty formation and international rule making surrounding the adaptation of these standards to the internet age.

Questions for potential discussion:

(1) How can we address the democratic deficits that result from one state's legislature or court, or one corporation, imposing rules and balances, on the rest of the world without the 'consent of the governed'?

(2) Does existing conflict-of-laws rules, such as the rule of comity, offer courts sufficiently clear doctrinal tools to resolve these tensions? Over the past few years, different commentators have proposed different tests for adjudicative comity in cyberspace. Amongst those are the following proposals. Which of these is most appealing? Are there additional proposals? Are these proposals impractical or ineffective?
    a. Whether the order sought would offend a third State's core values or important interests (amongst others human rights, national security, public order, public health, morals, economic well-being);
    b. The extent to which non-issuance of the order would result in undermining core values or important interests of the forum state;
    c. Whether the "balance of equities" favors the issuance of the order;
    d. Whether the order is proportionate, and whether there are less intrusive means of achieving the aim sought;
    e. Whether conducting a comity analysis would be futile in light of the specific circumstances of the case;
    f. Whether the substantive laws (be them rules of intellectual property, data protection, civil or criminal procedure) of the affected states conflict or whether they can be interpreted harmoniously;

(3) Which party should be tasked with establishing the existence and scope of the conflict: the party seeking the order, the party refusing the order, the court issuing the order, the court enforcing the order? What are the evidentiary standards necessary for establishing a conflict, in the context of disputes over data? Under what circumstances can the burden be shifted? (particularly in the context of courts asking litigants to show that enforcing the order would actually result in violation certain foreign laws, and the burden it creates on those litigants).

(4) Under what circumstances, and for what reasons, can a court in one jurisdiction refuse to enforce the global order of a court in another jurisdiction, as it relates to conflicts in the information society? How can we advance inter-operability between different actors? How can we ensure the development of future regulation will take into account the needs and interest of an array of stakeholders?

(5) Is there a need for a "Digital Geneva Convention"? What can such a convention look like from the perspective of jurisdictional conflicts in the information society? What areas should and shouldn't it cover?

(6) Given the growing public functions that certain corporate actors are playing, in what ways should traditional public and private international law standards be extended onto them?

Appendix C: Suggested Readings

All readings are accessible via a shared google drive (available at: goo.gl/UFgxPd).

The Internet and Jurisdiction (I&J) Policy Network offers a database, updated monthly, with brief summaries and major developments surrounding such cases and legislation worldwide which might be of relevance to workshop participants. The I&J database can be accessed at goo.gl/Qn3GBB. We further recommend reviewing some of the work done at the Institute for Information Security and Privacy at Georgia Tech, as part of their Cross-Border Requests for Data Project. The project website can be accessed at goo.gl/jZPkfa.

Theoretical Underpinnings

1. David Johnson and David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 Stanford Law Review 1367 (1996).
2. Jack Goldsmith, *Against Cyberanarchy*, University of Chicago Law Occasional Paper, No. 40 (1999).
3. David Post, *Against 'Against Cyberanarchy'*, 17 Berkley Technology Law Journal 1365 (2002).
4. Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale Law Journal 326 (2015).
5. Andrew Woods, *Against Data Exceptionalism*, 68 Stanford Law Review 729 (2016).
6. Dan Svantesson, *Against 'Against Data Exceptionalism'*, 2 Masaryk University Journal of Law and Technology 1 (2016).
7. THE NET AND THE NATION STATE, Introduction (Uta Kohl ed., 2017).

Mapping of the Existing Discourse

1. Council of Europe Commissioner for Human Rights, The Rule of Law on the Internet in the Wider Digital World, Issue Paper (2014).
2. Michael J. Reymond, *Hammering Square Pegs into Round Holes: The Geographical Scope of Application of the E.U. Right to be Delisted*, Berkman Klein Center Research Publication (2016).
3. Bertrand de La Chapella & Paul Fehlinger, *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*, Global Commission on Internet Governance Paper Series (2016).
4. Vivek Krishnamurthy, *Cloudy with a Conflict of Laws*, Berkman Klein Center Research Publication (2016).
5. Internet and Jurisdiction Policy Network, Input Documents for Workstreams of the Second Global Internet and Jurisdiction Conference (2017)
    a. Policy Options for Cross-Border Access to User Data
    b. Policy Options for Cross-Border Content Restrictions
6. Stanford Center for Internet and Society, Law Borders and Speech: Proceedings and Materials (Daphne Keller ed., 2017).
7. Peter Swire, *Why Cross-Border Government Requests for Data Will Keep Becoming More Important*, Lawfare (May 23, 2017).

8. Kurt Wimmer, *Free Expression and E.U. Privacy Regulation: Can the New GDPR Reach U.S. Publishers?*, 68 Syracuse Law Review 547 (2018).

Proposals for Regulatory Solutions

1. Donald Earl Childress, *Comity as Conflict: Resituating International Comity as Conflict of Laws*, 44 University of California Davis Law Review 11 (2010).
2. DAN JERKER B. SVANTESSON, SOLVING THE INTERNET JURISDICTION PUZZLE (2017).
3. United States v. Microsoft Corporation, Brief for Amici Curiae E-Discovery Institute *et. al.* in Support of Neither Party (2017).
4. Jennifer Daskal, *New Bill Would Moot Microsoft Ireland – And Much More!*, Just Security (Feb. 6, 2018).
5. Andrew Woods & Peter Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE Blog (Feb. 6, 2018).
6. Jennifer Daskal, *Borders and Bits*, 71 Vanderbilt Law Review 179 (2018).
7. Andrew Woods, *Litigating Data Sovereignty*, 128 Yale Law Journal 328 (2018).