This article was originally published on
Observer Research Foundation on October 14, 2016.

JURISDICTION ON THE INTERNET: HOW TO MOVE BEYOND THE LEGAL ARMS RACE

BY BERTRAND DE LA CHAPELLE AND PAUL FEHLINGER

The transborder nature of the Internet has generated unprecedented social, economic, and political benefits for humankind. At the same time, it creates tensions within an international legal system based on a territorial sovereignty principle rooted in the 17th century Treaty of Westphalia. On the Internet, transnational interactions have become commonplace. Traditional modes of interstate cooperation, therefore, struggle to cope with the digital realities of the 21st century. From cases of objectionable content to cross-border access to user data, online disputes and abuses are an unprecedented challenge to the territorially-bound international legal system.

We are confronted with two major questions: how can the global nature of cyberspace be preserved while respecting national laws? And how can misuse of and abuse on the Internet be addressed while ensuring the continued protection of human rights?

This represents acute concerns for all stakeholders, who are pressured to act yet lack the necessary tools to implement and enforce solutions. As a result, issues of jurisdiction on the Internet have engendered uncoordinated and unrestrained applications of territoriality online. Innovative processes are needed to fill the institutional gap in Internet governance and prevent the present legal arms race from escalating in their absence.

NATIONAL JURISDICTIONS AND TRANSBORDER CYBERSPACES

The technical architecture of the Internet was conceived as transborder and non-territorial from the onset, a quality that is generally regarded as advantageous. Yet ubiquity has also fostered tensions, as globally accessible content and services legal in one country may be illegal or even criminal in another. Historically, interactions across borders were rare exceptions. Today, most daily activities on the Internet involve multiple jurisdictions at once, allowing ample possibilities for conflicting laws to come into contact.

Determining applicable laws, allowing for their enforcement, and providing mechanisms for redress in cases of transborder cybercrime or illicit behaviour online becomes increasingly difficult as a result. Such tensions will continue accumulating as Internet penetration approaches four billion users from over 190 countries, each with divergent and potentially conflicting laws, cultures, and social sensitivities. The present situation is

a concern for all categories of actors: governments, Internet platforms, technical operators, civil society groups, and international organisations, as well as average users.

In addition to concerning a range of different actors, the jurisdictional challenge of Internet governance directly impacts other policy challenges. These include, among others, developing global digital economies, providing clear and predictable legal environments, protecting the exercise of fundamental human rights, and ensuring cybersecurity and public order. The active involvement of numerous actors and sectors is necessary to resolve jurisdictional tensions online and prevent the fragmentation of the Internet. Recognising the magnitude of this challenge is the first step toward finding a common solution.

Since 2012, the global multistakeholder policy network Internet & Jurisdiction has documented in its Retrospect publication more than 1000 high-level cases illustrating this growing tension, and engaged more than 100 key entities from all stakeholder groups in an ongoing dialogue process to address these issues and catalyse solutions. More than four years of global discussions in over 30 countries have allowed participants to identify three areas that dearly call for multistakeholder cooperation:

- Data. Under which conditions can public authorities in one country obtain user information from an operator in another jurisdiction? How can the right to privacy be reconciled with the need for lawful access to user data?

- Content. How can the global availability of content be maintained while handling the diversity of local laws and norms regarding speech? How can proportionality and respect of human rights be ensured in instances of content takedown?

- Domains. How do jurisdictions apply the Domain Name System, and how can the architectural separation between the Internet's application and logical layers be preserved?

In these and other complex issue areas, a lack of coordination between actors can result in unintended consequences and make problems harder – rather than easier – to solve.

A LEGAL ARMS RACE IN CYBERSPACE?

Digital sovereignty is becoming the realpolitik of Internet regulation. Examples of extraterritorial extension of national jurisdictions abound: first, governments with Internet platforms or technical operators incorporated on their soil may impose their national laws and regulations on these private actors, with direct transboundary impacts on all foreign users of these services. At the same time, draft legislations increasingly include clauses establishing extraterritorial reach, such as the draft UK Investigatory Powers Bill or the EU General Data Protection Regulation.

Litigation also plays a prominent role in setting new global standards, with de facto impacts far beyond the respective jurisdictions. Although the right to be de-indexed was originally established by Europe for Google, for example, it is now implemented by other search engines such as Microsoft Bing or Yahoo

Search and has produced ripple effects in Asia, Latin America, and Canada. Accordingly, local court decisions can also trigger new international norms for interactions between states and Internet companies.

Re-nationalization is a complementary trend to extraterritorial expansions of sovereignty. Courts and public authorities in countries that do not physically host Internet companies or data experience a sense of powerlessness when trying to levy respect for their national laws on foreign entities. Prompted to nevertheless establish the rule of law and protect citizens online, states are incentivised to erect territorial borders on the Internet. This can manifest itself through "data localisation" laws or the blocking of URLs (uniform resource locators) or IP (Internet protocol) addresses via the national Internet service providers (ISP). Other digital sovereignty measures can range from strong intermediary liability regimes, requirements to open local offices, demanding backdoors to encryption technologies, or the imposition of full-fledged licensing regimes.

The extreme and unrestrained leveraging of territorial criteria introduces two paradoxes. First, as described above, national actions impacting operators with global reach can affect citizens of other jurisdictions. Consequently, such actions appear contrary to the very principle of non-interference – a direct corollary of sovereignty itself. Such interference increases the potential for conflicts between jurisdictions, rewarding the most powerful digital countries and encouraging others to react and adopt measures based on mistrust and the reimposition of national borders.

Second, strong digital sovereignty measures are not scalable globally. Regarding compulsory data localisation laws, for example, it is highly unlikely that the necessary data centers could be established by global companies in every country around the world. Though sovereignty remains definitely relevant in the digital age, measures of extraterritorial expansion or renationalisation put actors in a classic prisoner's dilemma where the sum of actions appearing beneficial in the short-term can have unintended detrimental consequences for the future. In the case of Internet jurisdiction, the outcome of this negative-sum game is unwanted fragmentation and increasing conflicts. Preserving the global nature of the Internet and preventing a legal arms race to establish digital sovereignty call for new mechanisms of transnational cooperation.

LIMITS TO INTERNATIONAL COOPERATION

Managing transborder online spaces poses systemic difficulties for the existing international system; existing mechanisms for legal interoperability often fall short in diffusing tension and resolving conflict. Three such tools being employed at present are:

1. Multilateral efforts
2. Bilateral agreements
3. Informal interactions between public and private actors across borders.

Multilateral efforts. Only rare actors advocate the idea of a global, all-encompassing Internet treaty that would harmonise relevant laws and solve the full range of cyber-cooperation issues. Moreover, treaty negotiations are notoriously long. Even the most extensive agreement to date tackling cybercrime, the Budapest Convention, was a lengthy process: if formal negotiations took "only" four years, more than a decade was required to put the topic on the agenda. In the end, though the Convention was signed by more

than 50 states around the world (excluding several large countries such as India and Brazil), some countries use the fact that it was initially elaborated within the Council of Europe as an argument against joining a regime in the drafting of which they had not participated.

In the last few years, many useful declarations have been developed within multilateral organisations at the level of general principles, showing some form of convergence. Still, none of them were able to move towards developing operationally implementable regimes.

MLATs. Historically, the bilateral mutual legal assistance treaties (MLATs) enabling government-to-government legal cooperation were negotiated to handle rare and rather exceptional cross-border criminal cases. However, now that transborder interactions have become commonplace on the Internet and most criminal evidence is digital and hosted by operators in foreign countries, this system is generally described as "broken." MLATs have at least four structural limitations:

- MLAT processes can take months or even years to be processed, making them ill equipped to handle the instant and viral spread of information on the Internet.
- MLATs are often limited to "dual incrimination" situations – cases that qualify as a crime in the jurisdictions of both requesting and receiving countries – an obstacle given the disparity of national legislations.
- Regardless of the physical location of actions or involved parties, the MLAT system de facto imposes the law of the recipient country over the law of the requesting one, even if there is no territorial connection to the latter other than the incorporation of the targeted platform or operator.
- Establishing such bilateral relations among more than 190 countries would require more than 15,000 arrangements, an outcome neither feasible nor desirable.

Direct public-private requests. In the absence of timely and appropriate frameworks for international cooperation, public authorities in one country are increasingly sending requests directly to private actors in other jurisdictions, such as Internet platforms, hosting companies, registrars, or registries. This is particularly common in instances of requests for user data, content takedowns, and domain seizures. The internal transparency reports of some major global Internet companies provide a snapshot of the rise of such requests. Though there is a lack of reliable data to show the overall magnitude of this new trend, the increase in the number of requests reflects an attempt to establish modalities of voluntary cooperation.

Direct public-private requests however pose several problems. First, private companies are forced to make determinations on sensitive, high-stakes issues regarding economic conduct, international diplomacy, public safety, freedom of expression, and other human rights issues through procedures and criteria that lack transparency and due process. This can be an especially difficult situation when compliance with a foreign request would contradict the law in the company's country of incorporation. Meanwhile, forgone requests can lead to tensions, or in extreme cases to compulsory data localisation or the blocking of entire platforms through national ISPs. Finally, while large global platforms can afford to allocate the necessary human and financial resources to managing requests, start-ups and medium-sized companies with globally available content and services struggle more considerably in these circumstances.

A DANGEROUS PATH: UNINTENDED NEGATIVE CONSEQUENCES

The lack of coordination and inability of the international system to provide adequate and scalable cooperation solutions produce a typical "prisoner's dilemma"—actors, employing the only tools available to them, make short-term decisions that appear in their immediate interest, despite such solutions being sub-optimal or even detrimental in the long-term. On a wider scale, the sum of uncoordinated unilateral actions by governments and private actors can have serious unintended consequences.

Economically, a legal arms race would decrease investment in start-ups and medium-sized companies because of legal uncertainty and risks of intermediary liability, thereby stifling innovation, competition, and growth. In terms of freedom of expression and other human rights, increased pressure on Internet companies to accept direct requests could lower due process protections and produce a "race to the bottom", all in the absence of viable mechanisms for transborder appeals and redress for harmed Internet users. Barring other options, actors may be tempted to regulate content by manipulating the technical architecture of the Internet, wielding shutdowns or leveraging the location of registries and registrars to impose national laws. Finally, cooperation across borders is an urgent necessity when tackling cybercrime, terrorism, and other security threats confronting the global community at large.

FILLING THE INSTITUTIONAL GAP

Traditional intergovernmental cooperation mechanisms are failing to provide appropriate solutions for the dilemmas of Internet governance, revealing an institutional gap that must be filled to adequately address these new challenges.

An important distinction to be made in this field is the difference between governance "of" the Internet and governance "on" the Internet. While governance "of" the Internet concerns protocols, standards, addresses, and other elements of technical architecture, governance "on" the Internet relates to the use of the Internet, in the applications and services that run on top of the physical and logical layers, as well as in the behavior of Internet users. Though the jurisdictional challenges discussed in this paper are primarily related to governance "on" the Internet, important lessons and possible solutions may be gleaned from the technical management of the Internet.

Over time, an ecosystem has emerged to handle governance "of" the Internet and enable the necessary technical interoperability that the global network requires. Organisations such as the Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C) develop Internet and Web standards, while Regional Internet Registries and the Internet Corporation for Assigned Names and Numbers (ICANN) respectively organise the allocation of IP addresses and domain names. This ecosystem of transnational institutions is fundamentally distributed – each entity administers a specific issue and has its own internal structure and procedures, with loosely coupled coordination among them.

Despite their differences, each of these institutions covers the five stages necessary for the development and application of governance regimes: issue framing, drafting, validation, implementation, and reviews. Based on the fundamental principle of fostering multistakeholder involvement, governance "of" the Internet has enabled it to expand beyond the ambit of its research background to serve several billion people and permeate almost all human activities.

By contrast, the institutional ecosystem addressing issues related to governance "on" the Internet is embryonic at best. The UN's Internet Governance Forum (IGF) is a touchstone of this nascent field, providing an annual venue for actors to identify challenges, share experiences, and present their work. Yet, despite its essential role and numerous national and regional spin-offs, the IGF still only covers the first stages of the policy-making cycle: agenda setting and issue framing. Beyond some noteworthy efforts to document best practices, no efficient mechanisms exist yet to produce, let alone implement and enforce, the needed transnational arrangements for governance "on" the Internet.

Considering the diversity and distributed nature of technical governance organisations, the solution for governance "on" the Internet is not necessarily the replication of a single model. Indeed, addressing the issue of jurisdiction on the Internet requires neither the creation of a new international organisation nor the attribution of this responsibility to a single existing one, as Internet issues are relevant to the mandates of numerous entities. Filling the institutional gap in Internet governance demands a more innovative approach.

CATALYSING ISSUE-BASED POLICY NETWORKS

The issues of jurisdiction on the Internet lie at the intersection of four policy areas: legal cooperation, economy, human rights, and cybersecurity. Developing transnational mechanisms for policy coordination in these complex arenas will require ongoing, multistakeholder, and issue-based processes.

Based on the experience of Internet & Jurisdiction in leading a pioneering global dialogue process on these challenges, several key factors for the success of such issue-based policy networks have been identified:

- Framing the problem as an issue of common concern for all actors
- Ensuring the neutrality of the convener and facilitation team/secretariat
- Involving all stakeholder groups: states, Internet platforms, technical operators, academia, civil society, and international organisations
- Engaging a critical mass of actors with sufficient diversity to be representative of the various perspectives and to implement potential solutions
- Constructing and expanding a global network of key actors
- Creating trust among heterogeneous actors and adopting a shared vernacular
- Combining small groups and public reporting on progress to make the process both manageable and broadly transparent
- Informing stakeholders about relevant trends around the world to foster evidence-based policy innovation
- Providing sufficient geographic diversity from the onset to allow scalability in the adoption of any emerging policy solution

TOWARD TRANSNATIONAL FRAMEWORKS

Norms and procedures developed through such multistakeholder processes can be considered as "policy standards." As transnational frameworks for cooperation, they can establish mutual commitments between the different stakeholders, with:

- clear distribution of responsibilities;
- specific norms, procedural mechanisms or guarantees; and
- clear decision-making criteria.

As new forms of transnational soft law, such operational governance frameworks can establish procedural interoperability and due process across borders to handle multiple jurisdictions on the Internet. They can also help reform existing modes of interstate cooperation (for example, the Mutual Legal Assistance system), or fill current governance voids that require the creation of new sets of norms and standards.

Implementation and enforcement of such policy standards can employ a combination of existing tools and cover the range from simple, best practices to strict normative obligations. Public and private actors have different options to operationalise these shared norms. States, for example, can reference policy standards in their administrative procedures, while Internet platforms and technical operators can do so in their terms of service. Multistakeholder policy standards can even be institutionally embedded in national laws, endorsed by international organisations, or enshrined in new international treaties.

Drawing lessons from the governance "of" the Internet, a major advantage of standards is their potential to scale. Multistakeholder policy standards are based on consensus among different stakeholder groups, which augments the likelihood of successful and efficient adoption. They can more easily be implemented across heterogeneous public and private governance systems, which is key to creating interoperability. Moreover, such policy standards can be improved and adapted more quickly than conventional treaties, allowing them to develop further as the Internet ecosystem evolves.

Preserving the global character of the Internet and its social, political, and economic benefits for the next generations to come requires more cooperation among all stakeholders. We need to collectively develop new legal frameworks that are as transnational as the Internet itself in order to ensure legal interoperability and due process across borders.

THIS ARTICLE ORIGINALLY APPEARED IN THE DIGITAL DEBATES: THE CYFY JOURNAL