CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 28 — APRIL 2016

Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation

Bertrand de La Chapelle and Paul Fehlinger

JURISDICTION ON THE INTERNET: FROM LEGAL ARMS RACE TO TRANSNATIONAL COOPERATION

Bertrand de La Chapelle, Paul Fehlinger

CHATHAM HOUSE
The Royal Institute of International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

This work was carried out with the aid of a grant from the International Development Research Centre (IDRC), Ottawa, Canada.

The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHORS

Bertrand de La Chapelle is co-founder and director of the Internet & Jurisdiction Project. He was a director on the Internet Corporation for Assigned Names and Numbers (ICANN) Board from 2010 to 2013. From 2006 to 2010, he was France's Thematic Ambassador and Special Envoy for the Information Society. In this position, he participated in all World Summit on the Information Society (WSIS) follow-up activities and Internet governance processes, including in particular the Internet Governance Forum, and was a vice-chair of ICANN's Governmental Advisory Committee. Between 2002 and 2005, he actively participated in the WSIS to promote dialogue among civil society, the private sector and governments. He is a graduate of Ecole Polytechnique, Sciences Po Paris and Ecole Nationale d'Administration.

Paul Fehlinger is co-founder and manager of the Internet & Jurisdiction Project. He is actively engaged in global Internet governance fora, speaking at venues such as the Internet Governance Forum, the Organisation for Economic Co-operation and Development, and The Council of Europe. Paul was appointed to the Advisory Network of the Global Commission on Internet Governance and to the Working Group on Rule of Law of the Freedom Online Coalition. He is also a participant in the Council of Europe Committee of Experts on Cross-border Flow of Internet Traffic and Internet Freedom, and the World Economic Forum's Future of the Internet Initiative. He holds a master's degree in international relations from Sciences Po Paris, was a scholar of the German National Merit Foundation and has also worked in journalism.

ACRONYMS

ccTLDs	country-code top-level domains
DNS	domain name system
G20	Group of Twenty
gLTDs	generic top-level-domains
ICANN	Internet Corporation for Assigned Names and Numbers
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISPs	Internet Service Providers
MLATs	mutual legal assistance treaties
OECD	Organisation for Co-operation and Development
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
WSIS	World Summit on the Information Society

EXECUTIVE SUMMARY

The cross-border Internet and its online spaces span a fragmented patchwork of national jurisdictions. As connectivity and Internet penetration increase, so do the conflicts between jurisdictions. Such conflicts challenge the Westphalian international system, and traditional modes of legal cooperation struggle to resolve these jurisdictional tensions. Extreme application of the principle of territoriality and the exertion of digital sovereignty put the global community on a dangerous path if employed on the global scale. If nothing is done, this legal arms race could lead to severe unintended consequences for the future of the global digital economy, human rights, the technical Internet infrastructure and security.

Twenty-first century digital realities challenge traditional modes of international legal cooperation, revealing an institutional gap in Internet governance that may be solved by drawing lessons from the technical governance of the Internet. Preserving the global character of the Internet, fighting illicit online behaviour, and establishing procedural interoperability and due process across borders demand innovative cooperation mechanisms that are as transnational as the Internet itself.

In order to properly address jurisdictional tensions such as cross-border access to user data, content takedowns, or domain seizures, this paper recommends the creation of issue-based multistakeholder policy networks to develop scalable solutions.

INTRODUCTION

"In managing, promoting and protecting [the Internet's] presence in our lives, we need to be no less creative than those who invented it. Clearly, there is a need for governance, but that does not necessarily mean that it has to be done in the traditional way, for something that is so very different."

Kofi Annan, then UN Secretary-General[1]

The topic of jurisdiction has become a core issue for debate on the future of the Internet. The Internet's cross-border nature has produced unprecedented benefits for mankind. But it also generates tensions between national legal systems based on the territoriality of jurisdiction, particularly when dealing with abuses on the global network and Internet-related disputes.

Rooted in the treaties of the Peace of Westphalia of the seventeenth century, our international system is based on the separation of sovereignties, and these traditional modes of interstate cooperation struggle to cope with the digital realities of the twenty-first century.

We are confronted therefore with two major challenges: how to preserve the global nature of cyberspace while respecting national laws, and how to fight misuses and abuses of the Internet while ensuring the protection of human rights. Both challenges require cooperation and clear procedures across borders to ensure efficiency and due process.

Since 2012, the Internet & Jurisdiction Project has provided a neutral dialogue space for a policy network comprising more than 100 key stakeholders from around the world to explore operational solutions for transnational cooperation on jurisdictional issues. This paper directly draws upon the insights emerging from this pioneering multi-stakeholder process.

It addresses successively:

- why these issues represent a growing concern for all stakeholders, who are under pressure to find rapid solutions as the uses and misuses of the Internet increase;
- the legal arms race produced by the uncoordinated and unrestrained application of territoriality;
- the struggle of traditional modes of international cooperation to deal with this situation, especially with regard to access to user data, content takedowns and domain seizures;

1 The UN Secretary-General's remarks at the opening session of the Global Forum on Internet Governance on March 24, 2004. www.un.org/sg/STATEMENTS/index.asp?nid=837.

- the resulting dangerous path that threatens to destroy the nature and benefits of the global network and the risks related to economy, human rights, infrastructure and security;
- the need to fill the institutional gap in Internet governance through innovative processes involving all stakeholder groups; and
- how to move toward transnational cooperation frameworks.

NATIONAL JURISDICTIONS AND CROSS-BORDER CYBERSPACES

Conflicting Territorialities

The technical architecture of the Internet was conceived as cross-border and non-territorial from the onset. The World Wide Web technically allows, by default, access to any link regardless of physical location, and social media platforms serve hundreds of millions of users in shared cross-border online spaces. This transnational nature of the Internet has generated unprecedented benefits for humankind, be they political, economic or social. In particular, it uniquely fulfills the promises of Article 19 of the Universal Declaration of Human Rights regarding access to information "irrespective of frontiers."

Yet, globally accessible content that is legal in one country may be illegal or even criminal in another. Like any human-made tool, the Internet is susceptible to misuse, and so, cross-border cybercrime develops. Moreover, online communication tools are increasingly used by criminals "in the real world," and access to information stored by Internet operators in other countries becomes essential in investigations.

From a historical perspective, cross-border interactions were rare, and international legal cooperation tools were designed to handle these exceptions. However, on the open Internet, interactions across borders are becoming the new normal. As a consequence, cross-border conflicts arise between users, the services they use, public authorities and any combination thereof. How to determine the applicable laws when interactions are transnational is becoming increasingly difficult, as the current international system is based on a patchwork of separate and territorially defined national jurisdictions.

Teresa Scassa and Robert J. Currie (2010) argue that, "put simply, because the Internet is borderless, states are faced with the need to regulate conduct or subject matter in contexts where the territorial nexus is only partial and in some cases uncertain. This immediately represents a challenge to the Westphalian model of exclusive territorial state sovereignty under international law."

At least four territorial factors can play a role in determining applicable law: the location of the Internet user(s); the location of the servers that store the actual data; the locus of incorporation of the Internet companies that run the service(s) in question; and, potentially, the registrars or registries through which a domain name was registered.

These overlapping and often conflicting territorial criteria make both the application of laws in cyberspace and the resolution of Internet-related disputes difficult and inefficient. The principles of separation of sovereignties and non-interference between states that underpin the international system often render court decisions difficult to enforce and prevent the cooperation across borders necessary to efficiently deal with misuses online.

Tensions arise and will only grow as Internet penetration reaches four or five billion users from more than 190 different countries with diverse and potentially conflicting national laws and social, cultural or political sensitivities.

A Challenge for All Stakeholders

The present situation is a concern for each category of actors.

Governments have a responsibility to ensure respect of the rule of law online, protect their citizens and combat crime. A sense of frustration prevails in the absence of clear standards on how to enforce national laws on the cross-border Internet. Law enforcement agencies in particular feel unable to conduct necessary investigations to stop transnational crime and misuses of the network. In a system based on Westphalian territoriality, the principle of separation of jurisdictions becomes an obstacle to international cooperation.

Global Internet platforms, which relied on terms of service early on to establish the jurisdiction of their country of incorporation, now have to handle — and interpret — the 190-plus different national laws of the countries where they are accessible. This is a particular challenge to start-ups and medium-sized companies. Faced with growing direct requests for content takedown or access to user data, they also fear losing the protection of the limited-liability regime they have enjoyed so far and becoming responsible for thousands of micro-decisions of a quasi-judiciary nature[2] with significant human rights dimensions and reputation risks.

Technical operators worry that the fundamental separation of layers that forms the basis of the Internet architecture becomes blurred. Registries and registrars in particular see increasing efforts to leverage the domain name system (DNS) as a content control tool with global

2 Jacques de Werra (2015) labelled this new phenomenon "massive online micro justice."

reach. Hosting providers and internet service providers (ISPs) are equally concerned.

Civil society groups around the world worry about a potential race to the bottom in terms of protection of freedom of expression and privacy and a perceived privatization of dispute resolution. **Average users** are confused by the legal uncertainty about what rules apply to their online activities and feel powerless to obtain predictable and affordable redress when harmed, as multi-national litigation is beyond their reach.

International organizations struggle because of overlapping thematic scopes, or a geographical remit that is not universal. Although some, such as the Council of Europe, the Organisation for Economic Co-operation and Development (OECD), and the United Nations Educational, Scientific and Cultural Organization (UNESCO) have made significant efforts to include civil society, the private sector and the technical community in their processes, they remain by nature intergovernmental organizations. As such, they are limited in their capacity to put sensitive but necessary issues on their agenda by the lack of consensus, or worse, dissent among their members.

A Core Issue of Internet Governance

The jurisdictional challenge is at the nexus of Internet governance and touches upon multiple traditional policy areas: the development of the global digital economy, ensuring a clear and predictable legal environment through cooperation, guaranteeing the exercise of fundamental human rights, and ensuring security and public order. Since 2012, the Internet & Jurisdiction Project's Observatory has documented more than 1,000 high-level cases around the world that show the growing tension between national jurisdictions[3] due to the cross-border nature of the Internet.

Contrary to what they may perceive, however, the different categories of stakeholders have less of a problem with each other than a problem in common — that is, how to manage the coexistence of different norms in shared online spaces. Realizing this is the necessary first step toward a common solution. As the World Economic Forum's 2016 report on Internet fragmentation shows, trends toward the re-nationalization of cyberspaces are observable (Drake, Cerf and Kleinwächter 2016). Maintaining a global Internet *by default*, which fulfills the ambitions of the Universal Declaration of Human Rights, notably article 19, and boosts innovation and growth through online services and the cloud economy, requires transnational legal cooperation.

Within the global Internet & Jurisdiction multi-stakeholder process, three key issues have emerged as potential areas for such cooperation:

- **Domain name seizures**: Under which conditions and criteria is action at the DNS level justified, given its global impact?
- **Content takedown and withholding**: How can stakeholders determine proportionate restrictions to access that respect both national laws and international human rights?
- **Access to user data**: Under which conditions can law enforcement in one country obtain communication of user information from a foreign operator?

In each case, both procedural and substantive elements need to be addressed to develop balanced regimes.

Unfortunately, unilateral actions by actors to solve the complex jurisdictional conundrum on their own create a legal competition that makes the problem harder, rather than easier, to solve.

A LEGAL ARMS RACE IN CYBERSPACE?

Solving the Internet and jurisdiction challenge is intrinsically linked to the general debate about modalities of global governance. Christoph Knill and Dirk Lehmkul (2002) already observed in 2002 that "[e]conomic and technological interdependencies have created a range of problems that exceed the scope of national sovereignty and can therefore no longer be sufficiently resolved by the unilateral action of national governments."

Yet, confronted with increasing domestic pressure to address cyber issues, governments feel compelled to act on their own, using an extensive interpretation of territoriality criteria. This "hyper-territoriality" manifests itself by either extending sovereignty beyond national frontiers or reimposing national borders.

Extraterritoriality

Extraterritorial extension of national jurisdiction is becoming the *realpolitik* of Internet regulation.

First of all, governments with Internet platforms or technical operators incorporated on their soil can impose their national laws and regulations on these private actors, with direct transboundary impacts on all foreign users of these services. An often-cited example regarding the United States is the surveillance capacities described in the Snowden revelations. Regarding the reach of law enforcement, an ongoing landmark lawsuit will determine whether US authorities have a right to access emails stored by Microsoft, a US company, in its data centres in the Irish jurisdiction.[4] Previous cases involved a Department

3 See the Internet & Jurisdiction Observatory Retrospect Archive (n.d.).

4 See Internet & Jurisdiction Retrospect (2015).

of US Homeland Security agency seizing domain names belonging to foreign registrants on the sole basis of their registration through a US-based registrar (the RojaDirecta case[5]) or registry (the Bodog case[6]).

Furthermore, draft legislations increasingly include clauses establishing extraterritorial reach, such as the UK Investigatory Powers Bill[7] or the General Data Protection Regulation in the European Union.[8]

Finally, litigation also plays a prominent role in setting new global standards, with impacts far beyond the respective jurisdictions. Facebook, for instance, changed its global terms of service after a US court decision on its "sponsored stories" feature.[9] Courts increasingly affirm competence regarding services incorporated in other countries merely because they are accessible in their territory, as illustrated by the recent Yahoo case in Belgium.[10] Some difficulties naturally exist in enforcing the resulting judgments, as the national blockade of WhatsApp in Brazil showed.[11] Yet local cases can have global impacts. For instance, after the Court of Justice of the European Union Costeja decision (the right to be de-indexed), the French data protection authority demanded that Google extend its de-indexing to all versions of its search engine, arguing that the service is based on a single processing of data worldwide.[12]

Local court decisions can also trigger new international norms for the interaction between states and Internet companies. For instance, the right to be de-indexed, initially established by Europe for Google, is now implemented by other search engines such as Microsoft Bing or Yahoo Search[13] and has produced ripple effects in Asia[14] and Latin America.[15]

Digital Sovereignty

Not all countries are able — or trying — to extend their sovereignty beyond their borders. As a consequence, re-nationalization is a complementary trend to extraterritorial extension of sovereignty. The theme of "digital sovereignty" gains traction in many jurisdictions in a context of rising tensions and a sense of powerlessness by public authorities to impose respect for their national laws on foreign-based Internet platforms and technical operators. This can mean efforts to literally re-erect borders on the Internet through blocking of uniform resource locators or Internet Protocol (IP) addresses via national ISPs — something that has become much easier to implement today than in the early 2000s — or the creation of a limited number of national gateways.

So-called "data localization" laws are also part of this trend. They range from indirect requirements that would impose data localization only as a last resort if companies fail to honour legitimate national requests (see Brazil's Marco Civil[16]) to strict requirements, which stipulate that the data of national citizens processed by foreign companies needs to be stored within the national jurisdiction (see Russia[17]).

Other digital sovereignty measures can range from strong national intermediary liability regimes,[18] requirements to open local offices, demanding back doors to encryption technologies or the imposition of full-fledged licensing regimes.

Paradoxes of Sovereignty

Extreme and unrestrained leveraging of traditional territorial criteria introduces two paradoxes.

First, as described above, national actions upon operators with global reach have impacts on other jurisdictions. Such actions appear contrary to the very principle of non-interference, which is a direct corollary of sovereignty itself. This increases interstate tensions and potential conflicts between jurisdictions. While rewarding the most powerful digital countries, it encourages others to react and adopt measures based on mistrust and the reimposition of national borders.

Second, strict digital sovereignty measures such as data localization are not scalable globally. It is highly unlikely that necessary data centres could be, for example, established in all developing or small countries. Furthermore, although often presented as a tool to prevent surveillance, it might increase the likelihood of surveillance through the replication of data, which is required to create local copies that are stored in the reach of national authorities, while still allowing global processing and cross-border interactions.

5 See Internet & Jurisdiction Retrospect (2012a).

6 See Internet & Jurisdiction Retrospect (2012b).

7 See Internet & Jurisdiction Retrospect (2016).

8 See Internet & Jurisdiction Retrospect (2015b).

9 See Internet & Jurisdiction Retrospect (2013).

10 See Internet & Jurisdiction Retrospect (2015c).

11 See Internet & Jurisdiction Retrospect (2015d).

12 See Internet & Jurisdiction Retrospect (2015e).

13 See Internet & Jurisdiction Retrospect (2015f).

14 See Internet & Jurisdiction Retrospect (2014a).

15 See Internet & Jurisdiction Retrospect (2015g).

16 See Internet & Jurisdiction Retrospect (2014b).

17 See Internet & Jurisdiction Retrospect (2015h).

18 For an overview of national intermediary liability regimes, see Stanford World Intermediary Liability Map at https://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap.

Sovereignty is relevant in the digital age, but it behooves governments to take into account the potential transborder impact of their national decisions. This is why the recommendation adopted in 2011 by the Committee of Ministers of the Council of Europe established the responsibility of states to avoid "adverse transboundary impact on access to and use of the Internet" when they enforce national jurisdictions (Council of Europe 2011).

Exercised without restraint, both "extraterritorial extension of sovereignty" and "digital sovereignty" measures run contrary to the Kantian categorical imperative that should underpin international Internet regulation: Any national policy measure that would be detrimental if generalized around the world should not be adopted in the first place. International norms of cooperation are needed to prevent this legal arms race.

LIMITS TO INTERNATIONAL COOPERATION

Managing cross-border commons poses systemic difficulties for the existing international system (Ostrom 1990). The Westphalian principles of separation of sovereignties and non-interference actually represent more of an obstacle than a solution for cooperation on cyber issues.

John Palfry and Urs Gasser et al. (2012) and Rolf H. Weber (2014) rightfully argue that we need more legal interoperability to preserve the global nature of the Internet, but substantive harmonization of laws related to the use of the Internet seems unattainable. Multilateral efforts have proved so far inconclusive; bilateral arrangements such as mutual legal assistance treaties (MLATs) are in dire need of reform; and the increasing number of informal interactions between public and private actors across borders lack procedural guarantees.

Obstacles to Multilateral Efforts

The Internet is by nature disruptive, including with respect to the international regulatory system. As A. Claire Cutler (2001, 133) puts it, "traditional Westphalian-inspired assumptions about power and authority are incapable of providing contemporary understanding, producing a growing disjunction between the theory and the practice of the global system."

The idea of a global, all-encompassing Internet treaty that would harmonize relevant laws and solve the full range of cyber-cooperation issues is advocated only by some rare actors, who have tried to draw an analogy to decades-long efforts of international negotiations that resulted in the Law of the Sea Convention or the Outer Space Treaty. But the Internet is not a natural commons and, as Wolfgang Kleinwächter (2001) has argued, "while all these international conventions can be seen as great achievements of contemporary international law, it is hard to believe that this is a usable model for policy and law-making for the global Internet" due to the newness, volatility and rapid pace of innovation in the digital realm (Nye 2014).

Since the end of the World Summit on the Information Society (WSIS), intergovernmental discussions in various UN fora have made little progress beyond the wording of the Declaration adopted in Tunis in 2005. Moreover, the international community was split in 2012 during the World Conference on International Telecommunications, signifying the absence of global consensus not only at the level of substance, but even on the proper institutional framework for such discussions.

In any case, 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 necessary to actually put the topic on the agenda. Although now signed by more than 50 states around the world (excluding, however, several large countries such as Brazil and India), some countries use the fact that it was elaborated initially within the Council of Europe as an argument to refuse joining a regime they did not participate in drafting. The Budapest Convention also require signatories to transpose its provisions into national laws and its Article 18 on "subscriber information" or Article 32b addressing "trans-border access to stored data" are often considered not sufficient enough to provide effective cooperation. Like all international agreements, the Budapest Convention is also difficult to modify in response to rapidly changing technology.

In the past few years, many useful declarations have been developed within multilateral organizations at the level of general principles, showing some form of convergence. Still, none of them were able to move toward developing an operationally implementable regime.

MLATs: The Switched Network of International Cooperation

Historically, the so-called MLATs enabling government-to-government legal cooperation were negotiated to handle rare and rather exceptional cross-border criminal cases. These intergovernmental tools allow public authorities in country A to ask for assistance to, for instance, access user data stored by an operator in country B. Upon receipt of the request, country B examines if it is also valid according to its national laws. If so, the data holder in country B is lawfully compelled to submit the data to authorities in country B, which will then share it with the requesting authorities of country A.

However, now that cross-border is the new normal on the Internet, this system is generally described as "broken." MLATs have at least four structural limitations:

- **Speed**: MLATs are ill adapted to the speed of the Internet and the viral spread of information. In the best cases, an MLAT request from one government to another takes months to be processed. It can take up to two years between certain countries. The very elaborate circuit of validations is legitimately intended to provide procedural guarantees, but makes the whole system impracticable.
- **Scope**: MLATs are often limited to "dual incrimination" cases, that is, they cover only issues qualified as a crime in the jurisdictions of both requesting and receiving countries. Given the disparity of national legislations, their relevance is limited, particularly on speech issues (such as hate speech and defamation). They are also ineffective when the location of the data is unknown.
- **Asymmetry**: Regardless of the actual physical location of events 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 other territorial connection to the latter than the incorporation of the targeted platform or operator. An increasing number of countries find this unbalanced, given the dominant role of US-based companies.
- **Scalability**: The system of traditional MLAT treaties can hardly encompass the scale of the Internet. A large number of countries around the world do not have MLAT treaties with each other, and establishing such bilateral relations among 190 countries would require more than 15,000 arrangements.[19]

The MLAT system is the switched network of international cooperation.[20] It is in dire need of reform to adapt to the Internet age and reforming it will not be easy. It will require more than simply streamlining existing procedures: creative solutions are needed to address its structural limitations and ensure both transnational due process and efficiency.

Recent initiatives have been launched in the United States, in particular to address the asymmetry issue, including a potential reform of the Electronic Communications Privacy Act of 1986. This represents a positive signal and international discussions are ongoing. The question of scope, however, remains, and many issues cannot be addressed via the MLAT approach as long as national legislations remain unharmonized.

The Rise of Direct Public-Private Requests Across Borders

In the absence of appropriate international cooperation frameworks, there are an increasing number of requests that public authorities in one country directly send to private actors in other jurisdictions, for the following three actions:

- **Domain seizures**: Removal of the entire domain of an allegedly infringing website.
- **Content takedown**: Removal or withholding of a specific piece of infringing content.
- **User data access:** Access to user information related to who posted infringing content, or other investigations.

There is a lack of reliable data to show the entire magnitude of this new trend. Transparency reports of some major global Internet companies provide a snapshot of the rise of such requests, but without sufficient harmonization of reporting methodologies. So far, only a small number of — mostly US-based — Internet companies publish such reports. Aggregated data from states, that is, the senders of these requests, is still unavailable. It is also important to understand that the original sending countries of MLAT requests are not revealed in such transparency reports, as these requests are ultimately handed down to companies as national requests from their respective countries of incorporation.

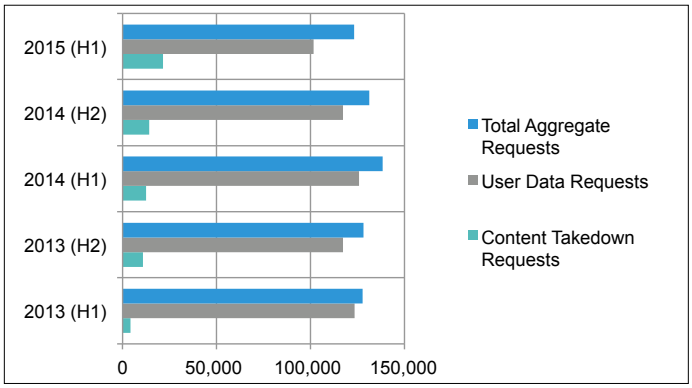
Pioneered by Google in 2009, transparency reporting is still a nascent trend. For example, nine out of the 13 analyzed platforms only launched transparency reports in 2013. Nevertheless, Figure 1 provides an indicative statistical overview by showing a survey of the combined number of requests received from public authorities (courts, law enforcement, other agencies) as reported by 13 Internet platforms[21] for content takedown and user data between 2013 and mid-2015.

19 For an overview of existing MLAT treaties, consult the MLAT Map by the non-governmental organization Access Now, available at https://mlat.info/.

20 For a comparison between the public switched telephone network and the distributed architecture of Internet routing see Internet Society (n.d.).

21 Combined data from transparency reports between 2013 and the first semester of 2015 on content takedown request (excluding copyright) and user information requests issued by governments (law enforcement, courts, other authorities) as reported by AOL (transparency reporting since 2011), Apple (since 2013), WordPress (since 2013), Dropbox (since 2013), Facebook (since 2013), Google (since 2010, although reports started in 2009), LinkedIn (since 2011), Microsoft (since 2013), Pinterest (since 2013), Snapchat (since 2014), Tumblr (since 2013), Twitter (since 2012), Wikimedia (since 2012) and Yahoo (since 2013).

Figure 1: The Rise of Direct Requests



Data sources: See footnote 22.

Note: H1 = first half of year, H2 = second half of year

Since 2013 the surveyed platforms reported in total 648,544 content removal requests (excluding copyright-related requests) and user information requests. The vast majority of reported requests have been addressed to four companies: Facebook, Google, Microsoft and Yahoo. The actual volume of such requests around the world is estimated to be much higher and will certainly rise with the next billion Internet users from increasingly diverse jurisdictions as they start using numerous Internet platforms and services.

Just in the first six months of 2015, Facebook (2015), for example, received requests from courts, law enforcement or other authorities from 92 jurisdictions, Google (2015) from 91 jurisdictions, Microsoft (2015) from 64 jurisdictions, Twitter (2015) from 37 jurisdictions and Yahoo (2015) from 34 jurisdictions.

This trend reflects an effort to establish modalities of voluntary cooperation between public and private actors across borders. However, it forces private entities to make determinations on sensitive high-stake issues regarding freedom of expression, human rights, economic conduct, international diplomacy and public safety through procedures and criteria that lack transparency and due process. It also often places them in a difficult situation, as when accepting a request conflicts with the law of their country of incorporation (for instance, direct communication of user content is prohibited by the Electronic Communications Privacy Act in the United States). Meanwhile, requests not honoured can lead to tensions or, in extreme cases, to the blocking of entire platforms by national ISPs or forced data localization. While world-leading platforms can afford to allocate the necessary human and financial resources, start-ups and medium-sized companies with globally available content and services have a greater struggle with this situation.

A DANGEROUS PATH

The lack of coordination and the inability of the Westphalian international system to provide the necessary cooperation solutions produce a typical "prisoner's dilemma" situation. That is, every single actor, forced to use the only tools available to it, makes short-term decisions that appear in its immediate interest, though their cumulative effect is at best suboptimal and most likely detrimental to all in the longer term.

If we continue to lack appropriate cooperation mechanisms and "fall back into managing the national, rather than managing shared cross-border online spaces in a collaborative way" (Fehlinger 2014), the sum of uncoordinated unilateral actions by governments and private actors can have unintended consequences, with strong negative impacts in economic, human rights, infrastructure and security areas.

Unintended Consquences

ECONOMY	HUMAN RIGHTS
Demise of globally accessible services	Reduced freedom of expression across borders
Market entry barriers	Limits to access to information
Reduced investment in start-ups	Limits to freedom of assembly in cross-border online spaces
Stifled innovation	Lack of access to justice and redress
Disadvantages for developing countries	
INFRASTRUCTURE	**SECURITY**
Blurred separation of layers	Eroding of global cyber security
Facilitation of surveillance	Diplomatic tensions
Encryption wars	Increase of cybercrimes and online terrorism
Restrictions to the use of virtual private networks	Threats to human security
Reduced network resilience	

Source: Author.

Economic Impacts

In 2014, the Boston Consulting Group estimated the value of the digital economy of the Group of Twenty countries alone at US$4.2 trillion, representing 5 to 9 percent of total GDP in developed countries (Boston Consulting Group 2014). The cross-border nature of the Internet and its cloud-based services are at the heart of innovation and growth. This is why the OECD is addressing the challenges to Internet openness in its June 2016 Ministerial Conference in Mexico and why the 2016 World Economic Forum's Davos meeting discussed the impact of cyberspace fragmentation. A legal arms race and lack of cooperation would stifle innovation and competition, and jeopardize

growth. Most established Internet companies were able to scale up internationally before the current move toward re-territorialization. The future development of global services and the cloud approach are at stake.

Investment in start-ups and medium-sized companies (especially those dealing with user-generated content) would decrease because of higher intermediary liability risks and legal uncertainty. Compulsory data localization might constitute a potential market entry barrier. Such requirements could be respected only by large, already established operators, limiting innovation and market accessibility for small companies wanting to serve a global market, particularly from developing countries.

Human Rights Impacts

International organizations such as UNESCO ("Internet universality") or the Council of Europe ("cross-border flow of Internet traffic and Internet freedom") have established the connection between human rights and the cross-border Internet (UNESCO 2013; Council of Europe 2015). It has uniquely fulfilled the promises of Article 19 of the Universal Declaration of Human Rights, allowing everyone to "seek, receive and impart information and ideas through any media and regardless of frontiers" (UN Human Rights Office of the High Commissioner (2011). enriched the social fabric across borders and improved our quality of life. Personal communication capacities are augmented, allowing frictionless expression, deliberation, and the holding of opinions across borders. The cross-border Internet facilitates the sharing and pooling of resources, and provides diasporas with irreplaceable communication tools. It has enabled the creation of critical-mass communities with common interests for social, political, or economic issues regardless of spatial distance and facilitated collaborative not-for-profit activities that have created tremendous global social value, such as Wikipedia.

The uncontrolled reterritorialization of the Internet in order to address its misuses could destroy the unprecedented human rights benefits the Internet has generated. Ironically, measures such as data localization and decryption could in fact increase opportunities for surveillance rather than reduce them, as well as harm the right to privacy (UN Human Rights Office of the High Commissioner 2015). Increased pressure on Internet companies to accept direct requests could produce a "race to the bottom" by limiting freedom of expression and lowering due process protections. Conversely, the continued absence of affordable cross-border appeal and redress mechanisms for harmed Internet users has a serious negative impact on global justice.

Technical Infrastructure Impacts

In 2013, the leaders of the 10 organizations responsible for coordination of the Internet's technical infrastructure met in Montevideo, Uruguay, to stress in their joint statement "the importance of globally coherent Internet operations, and warned against Internet fragmentation at a national level"(Internet Corporation for Assigned Names and Numbers [ICANN] 2013). In enforcing national laws online in the absence of international cooperation frameworks, there is a temptation to use the technical infrastructure of the Internet to address content issues. This, however, blurs a fundamental architectural principle of the Internet: the separation of the neutral logical layer (DNS, IP addresses, et cetera) and the application layer (online platforms and services).

Leveraging the location of registries and registrars to impose the national laws of their country of incorporation on the global content under the country-code top-level domains (ccTLDs) or generic top-level-domains (gTLDs) they manage would be a clear extraterritorial extension of sovereignty, given the global impact of a domain seizure. In parallel, generalizing geo-IP filtering to withhold content on specific territories may lead to forcing Regional Internet Registries to systematically allocate IP addresses on a territorial basis. Such a scenario could complicate routing. With the transition from IP version 4 (IPv4) to IP version 6 (IPv6), it could even facilitate surveillance, should IP addresses be permanently hardwired to specific devices and become identity identifiers.

In an effort by Internet companies to reduce their multi-jurisdictional liability, unbreakable encryption technologies might lead to a spiral of encryption/decryption conflicts between public and private actors. The imposition of a limited number of Internet gateways to connect a territory in order to facilitate blocking measures potentially reduces the resilience of the overall technical network. Finally, the banning of technologies such as virtual private networks is not only contrary to Article 13(2) of the Universal Declaration of Human Rights,[22] it also reduces the security of transactions and communications.

Security Impacts

The absence of agreed-upon frameworks to handle requests across borders has already resulted in diplomatic tensions between a country seeking to enforce its national laws and the country in whose jurisdiction the Internet platform or technical operator is actually located. Examples are Google's China exit in 2010 (McCullagh 2010), the Indian

22 Universal Declaration of Human Rights Article 13(2): "Everyone has the right to leave any country, including his own, and to return to his country."

Assam riots in 2012,[23] the Innocence of Muslim YouTube video in 2012[24] and Turkey's blocking of Twitter in 2014.[25] Likewise, debates about MLAT reform are fuelling interstate dissonances. Such international conflicts are likely to increase if nothing is done.

It is the duty of states to protect their citizens and maintain public order within the provisions of Article 29 of the Universal Declaration of Human Rights. However, the rapid and viral propagation of incitation to violence (often called "digital wildfires") could lead to disaster if we lack efficient transnational cooperation mechanisms that set standards and procedures for the interactions between states, Internet platforms and users across borders in situations of public order tensions. The international fight against terrorism online is emblematic of this challenge. Meanwhile, cybercrime is on the rise, and most online crimes have a multi-jurisdictional footprint, which makes cooperation across borders necessary to guarantee the security online, as well as off-line. The absence of appropriate regimes to access data across borders further increases the incentives for direct surveillance. Failure to develop the needed frameworks might ultimately lead to a decrease in global cyber security and order.

FILLING THE INSTITUTIONAL GAP IN INTERNET GOVERNANCE

Traditional intergovernmental cooperation mechanisms are failing so far to provide appropriate solutions. Legal harmonization on substance is difficult to achieve but the costs of inaction are daunting. There is an institutional gap in the Internet governance ecosystem that must be filled to adequately address these new challenges. In doing so, following the words of former UN Secretary-General Kofi Annan, we need to be as creative as the inventors of the Internet. To preserve the global nature of the Internet and address its misuses demands the development of innovative cooperation mechanisms that are as transnational, inclusive and distributed as the network itself.

Lessons from the Technical Governance "of" the Internet

Internet governance was famously defined in the United Nation's WSIS Tunis Agenda (2005) as "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."

In this definition, we see a distinction between governance "of" the Internet and governance "on" the Internet (de La Chapelle 2007). Governance "of" the Internet designates the governance of protocols, standards, addresses and *the evolution* of the technical architecture. Governance "on" the Internet relates to *the use* of the Internet, that is, the applications and services that run on top of the physical and logical layers, as well as Internet users' behaviour. The jurisdictional challenges discussed in this paper are primarily related to governance "on" the Internet.

A complex and robust network of institutions has emerged over time to handle governance "of" the Internet. It comprises, *inter alia*, the Internet Engineering Task Force and World Wide Web Consortium (W3C) for the development of Internet and web standards; five Regional Internet Registries allocating IP addresses; the 13 root servers and their multiple mirrors; ICANN; and the numerous registries and registrars distributing second-level domain names.

In dealing with the Internet's logical layer, each of these institutions covers the five stages necessary for the "development and application" of governance regimes: issue-framing, drafting, validation, implementation and reviews. The policies developed through their bottom-up participatory processes can have wide-ranging transnational implications, such as when ICANN regulates the allocation of the semantic spectrum of gTLD extensions or the accreditation of market operators (registrars and registries).

Together, these institutions formed the necessary ecosystem of governance that has enabled the Internet to grow from the limited ambit of its research background to serve several billion people and permeate almost all human activities. This ecosystem of transnational institutions is fundamentally distributed; each entity deals with a specific issue, with loosely coupled coordination. It was developed progressively through time as policy needs arose. Each entity has its own specific institutional structure and internal procedures. Most important, they operate on a fundamental principle: the open participation of all relevant stakeholders in the processes dealing with issues they impact or are impacted by.

Evolution of the Ecosystem: Governance "on" the Internet

By contrast, the institutional ecosystem addressing issues related to governance "on" the Internet is embryonic at best, or as Mark Raymond and Laura DeNardis (2015) elegantly expressed, "inchoate."

The IGF is the main outcome of the WSIS process. In its 10 years of existence, it has demonstrated its capacity to act every year as a "watering hole," where all actors identify challenges, share experiences and present their work.

23 See Internet & Jurisdiction Retrospect (2012c).

24 See Internet & Jurisdiction Retrospect (2012d).

25 See Internet & Jurisdiction Retrospect (2014c).

However, despite its undeniable success and essential role, not to mention the emergence of numerous national and regional spinoffs, it still only covers at best 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 enable ongoing intersessional work on specific issues to produce, let alone implement and enforce, the needed transnational arrangements for governance "on" the Internet.

The NETmundial Roadmap, an outcome of the major 2014 multi-stakeholder conference, highlighted the jurisdiction issue as an important topic for the global community (NETmundial 2014). To preserve the cross-border nature of the Internet by default for the next generations to come, we need to collectively fill the institutional gap for the governance "on" the Internet. This is in line with the ambitions of the global Internet governance community to "further develop the Internet governance ecosystem to produce operational solutions for current and future Internet issues," and to preserve the Internet as a "unified and unfragmented space" in a collaborative manner (NETmundial n.d.).

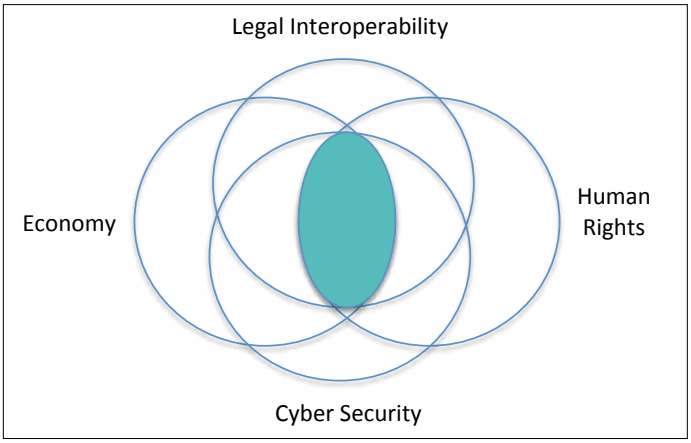
In doing so, we need to keep in mind the lessons that made the success of the existing institutional ecosystem for governance "of" the Internet. The robustness of the policies and solutions it produces is directly related to its fundamental characteristic of being transnational, open and organized in a distributed way. Given the diversity of the modes of organization of technical governance organizations, this does not mean the mere replication of a single model, but rather taking adequate inspiration from these principles to develop the governance "on" the Internet.

In the specific case of developing new transnational cooperation mechanisms for domain seizures, content takedowns and access to user data, the institutional gap of governance "on" the Internet lies at the intersection of four policy areas: legal interoperability, economy, human rights and cyber security (See Figure 2).

Enabling Issue-Based Multi-stakeholder Cooperation

The multi-stakeholder approach was explicitly endorsed by more than 180 countries at the heads of state level in the Tunis Agenda in 2005, and reconfirmed in the United Nations General Assembly High-Level Meeting on the WSIS+10 in December 2015. Filling the institutional gap requires neither the creation of new international organizations nor giving a unique responsibility to any existing one, as Internet issues are relevant to the mandates of a plurality of entities. A more creative approach is needed: the formation of issue-based governance networks.

Figure 2: Filling the Institutional Gap



Source: Authors.

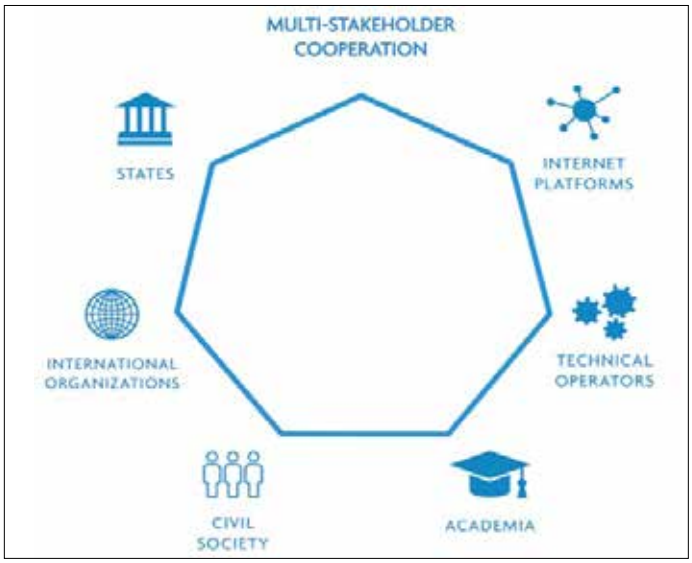
In line with the 2014 recommendations of the High-Level Panel on Global Internet Cooperation and Governance Mechanisms (ICANN 2014) chaired by the President of Estonia, Toomas Ilves, developing transnational mechanisms for policy cooperation requires ongoing, multi-stakeholder and issue-based processes:

- **Ongoing**, because the current proliferation of one-shot conferences, fora, panels and workshops, however useful to foster mutual understanding, is not sufficient to move toward operational solutions. Developing networks, trust and a common approach to issues and objectives cannot be achieved in disconnected series of two-hour sessions.

- **Multi-stakeholder**, because no single stakeholder group working alone can grasp all the technical, political, legal, security, social and economic dimensions of an issue — a condition for the development of balanced regimes. Furthermore, the likelihood of rapid implementation and scalability is increased if the diverse actors that will have to contribute to the implementations of a regime have also participated in its elaboration.

- **Issue-based**, because each topic involves different sets of concerned stakeholders, or even different individuals and units within each entity. Efficient policy innovation therefore requires focus on a specific issue to ensure inclusion of all relevant actors.

Figure 3: Six Stakeholder Groups



Source: Authors.

Based on the lessons of the Internet & Jurisdiction Project, some key factors for the success of such issue-based policy networks are:

- framing the problem as an issue of common concern for all actors;
- ensuring the neutrality of the convener and facilitation team/secretariat;
- involving all six stakeholder groups: states, Internet platforms, technical operators, academia, civil society, and international organizations (See Figure 3);
- 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 smaller working groups and reporting on progress to make the process manageable and transparent;
- informing stakeholders about relevant trends around the world to foster evidence-based policy innovation; and
- providing sufficient geographic diversity from the onset to allow the scalability of adoption of any emerging policy solution.

Addressing jurisdiction issues on the Internet and preempting the current legal arms race requires enhanced efforts to catalyze multi-stakeholder cooperation on the specific topics of cross-border requests for domain seizures, content takedowns and access to user data.

TOWARD TRANSNATIONAL FRAMEWORKS

Such innovative multi-stakeholder networks can produce scalable and adaptive policy standards that guarantee procedural interoperability and transnational due process in relations between public and private actors.

Procedural Interoperability

International human rights frameworks already represent an overarching substantive reference at the global level. Recent UN Human Rights Council (2014) resolutions have reaffirmed that they apply online as well as off-line. However, rapid substantive legal harmonization at a more detailed level regarding use of the Internet is unrealistic, given the diversity of legislations that are often considered strong elements of national identity. Meanwhile, cross-border requests for domain seizures, content takedowns and access to user data pose everyday problems that require urgent action, as the stakes involved are high.

In contrast to traditional interstate cooperation, these increasingly cross-border interactions engage heterogeneous public and private actors. They are conducted in all shapes and formats, through broadly diverse communication channels, and often without clear and standardized procedures or sufficient transparency. In that context, prioritizing the development of shared procedural standards has several benefits:

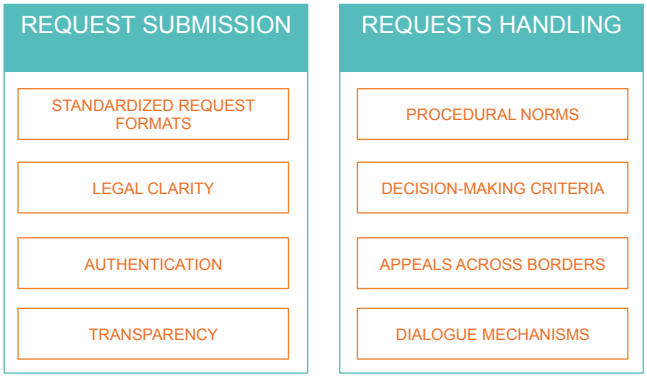
- It provides a field of cooperation that helps build trust among stakeholders and paves the way for constructive discussions on contentious substantive norms.
- It establishes interoperability among heterogeneous actors byproviding shared vernacular and mechanisms for their interactions, not unlike the Transmission Control Protocol/IP enabled interoperability between heterogeneous networks.
- It prepares a future digitization of the request treatment workflow, in order to reduce the delays that plague current mechanisms, such as MLATs.
- Most important, it is an opportunity to incorporate due process requirements in operational frameworks by design, in order to improve transnational interactions and safeguard users' rights across borders.

Transnational Due Process

After four years of international multi-stakeholder discussions facilitated by the Internet & Jurisdiction Project, key elements of transnational due process have been identified with the goal of providing avenues for best practices, improving existing mechanisms such as MLATs and identifying a potential architecture for novel cooperation frameworks.

This architecture for transborder requests deals with two aspects: how requests are submitted and how requests are handled (Figure 4).

Figure 4: Architecture for Transnational Due Process Frameworks



Source: Authors.

The submission of requests raises the following sets of questions:

- How can request formats be standardized? What are current best practices? How can we incorporate due process by design into such formats?
- How can we ensure legal clarity for both intermediaries — potentially subjected to 190-plus different jurisdictions — and for users who struggle to understand the rights and obligations that apply to them in cyberspace?
- How can we build trust between senders and recipients of cross-border requests through authentication, in order to avoid abuses and arbitrary requests?
- What are best practices for transparency reporting? How can we spread this practice among public and private actors to increase accountability?

How requests are handled addresses the following components:

- What procedural norms must be respected by senders and recipients to make requests legitimate?
- Which decision-making criteria can ensure the respect of human rights and guarantee proportionality?
- What procedures can allow affordable and efficient redress by parties, especially users, across borders?
- How can trusted and efficient communication channels be constructed across borders to mitigate escalating tensions between public and private actors, especially in cases of non-compliance with requests?

While each of these questions can be further broken down into sub-elements, they will not be described here, as the above list is intended principally as a framework for discussions.

Governance through Policy Standards

Norms and procedures developed through such multi-stakeholder processes can be considered "policy standards." As innovative transnational cooperation frameworks, 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, in the context of addressing jurisdiction on the Internet, guarantee procedural interoperability and due process. In doing so, they can either help to reform existing modes of interstate cooperation (for example, the MLAT system) or fill current governance voids that require new sets of norms and standards.

Implementation and enforcement of such policy standards can leverage 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 operationalize these shared norms through measures such as states referencing policy standards in their administrative procedures, or Internet platforms and technical operators doing so in their terms of service. Multi-stakeholder policy standards can even be institutionally embedded in national laws, endorsed by international organizations or enshrined in new international treaties.

Drawing lessons from the governance "of" the Internet, a major advantage of standards is their potential to scale. Multi-stakeholder 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 the key to creating interoperability. Moreover, such policy

standards can be improved and adapted more quickly than conventional treaties, which allows them to develop further as the Internet ecosystem evolves.

CONCLUSION

Thomas Kuhn, in his *Structure of Scientific Revolutions* (1962) , describes paradigm shifts that modify the model underpinning a particular field when it no longer reflects or correctly explains observations. The Copernican revolution in astronomy is the most familiar example, triggered by the observations of Galileo's telescope. Similarly, political paradigm shifts occur when a particular model of societal organization struggles to adequately address all problems of the time.

Rooted in the treaties of the Peace of Westphalia of the seventeenth century, our international system, based on the territorial jurisdictions, the separation of sovereignties, and non-interference, struggles to handle the transborder digital realities of the twenty-first century. The Internet acts like Galileo's telescope, showing that traditional principles and approaches can become as much an obstacle as a solution to address the jurisdiction challenge in cross-border online spaces.

Addressing issues related to governance "on" the Internet requires a paradigm shift: from international cooperation only between states, to transnational cooperation among all stakeholders; from pure intergovernmental treaties to policy standards; and from intergovernmental institutions to issue-based governance networks.

Far from a rejection of traditional international cooperation, however, this is proposed as a constructive extension — a way to look at current practices in a new, generalized light. In physics, two theories coexist at the same time: relativity theory applies at high velocities in space; but in normal conditions, classical Newtonian, equations still allow us to build bridges and predict trajectories. Both have their respective zones of validity. Likewise, the type of transnational cooperation envisioned here in no way suppresses or reduces the relevance and authority of existing governance frameworks, in particular national governments. On the contrary, multi-stakeholder processes can produce policy standards that inform the reform of existing interstate cooperation mechanisms, and policy standards can even later be enshrined by traditional multilateral organizations.

The global community needs to step up efforts to avoid the negative consequences of a legal arms race, preserve the global nature of the Internet and address its misuse. We need innovative cooperation mechanisms that are as transnational as the Internet itself and the necessary policy networks and ongoing dialogue processes to produce them.

WORKS CITED

Boston Consulting Group. 2014. *Greasing the Wheels of the Internet Economy.* https://www.icann.org/en/system/files/files/bcg-internet-economy-27jan14-en.pdf.

Council of Europe. 2011. *Recommendation CM/Rec (2011)8 of the Committee of Ministers to Member States on the Protection and Promotion of the Universality, Integrity and Openness of the Internet.*

———. 2015. *Recommendation CM/Rec(2015)6 of the Committee of Ministers to Member States on the Free, Transboundary Flow of Information on the Internet.* https://wcd.coe.int/ViewDoc.jsp?id=2306649.

Cutler, A. Claire. 2001. "Critical reflections on the Westphalian assumptions of international law and organization: a crisis of legitimacy." *Review of International Studies* 27 (02): 133–50.

de La Chapelle, B. 2007. "The Internet Governance Forum: How a United Nations Summit Produced a New Governance Paradigm for the Internet Age." In *Governing the Internet: Freedom and Regulation in the OSCE Region*, edited by OSCE, 27.

De Werra, Jacques. 2015. "Alternative Dispute Resolution in Cyberspace: Can ADR Address the Challenges of Massive Online Micro Justice?" Presentation at the University of Geneva, November 27. http://svir-ssdi.ch/fileadmin/user_upload/VR-Tage/SSDI_-_Jde_Werra_-_ADR__24_11_2015_.pdf.

Drake, W. J., V. G. Cerf and W. Kleinwächter. 2016. *Internet Fragmentation: An Overview.* World Economic Forum Future of the Internet Initiative White Paper. Geneva, Switzerland: World Economic Forum. www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

Facebook. .2015. Facebook Transparency Report. Government requests report January — June 2015. https://govtrequests.facebook.com/.

Fehlinger, P. 2014. "Cyberspace Fragmentation: An Internet Governance Debate beyond Infrastructure." Internet Policy Review. https://policyreview.info/articles/news/cyberspace-fragmentation-internet-governance-debate-beyond-infrastructure/266.

Google. 2015. Google Transparency Report. Requests for user information January — June 2015. https://www.google.com/transparencyreport/userdatarequests/countries/.

ICANN. 2013. "Montevideo Statement on the Future of Internet Cooperation." https://www.icann.org/news/announcement-2013-10-07-en.

———. 2014. *Towards a Collaborative, Decentralized Internet Governance Ecosystem: Report by the Panel on*

Global Internet Cooperation and Governance Mechanisms. Retrieved from www.internetsociety.org/sites/default/files/Internet%20Governance%20Report%20iPDF.pdf.

Internet & Jurisdiction. n.d. Internet & Jurisdiction Retrospect Archive. www.internetjurisdiction.net/observatory/.

Internet & Jurisdiction Retrospect. 2012a. "US authorities seize foreign .com gambling site registered in Canada via VeriSign." www.internetjurisdiction.net/observatory/retrospect/2012-february/.

———. 2012b. "US authorities give back seized domains of Spanish Rojadirecta site." www.internetjurisdiction.net/observatory/retrospect/2012-august/.

———. 2012c. "India cracks down on online content that stirs violence in its jurisdiction, needs US assistance to trace origins." www.internetjurisdiction.net/observatory/retrospect/2012-august/.

———. 2012d. "Pakistani YouTube block remains intact due to absence of MLAT with US jurisdiction." www.internetjurisdiction.net/observatory/retrospect/2012-november/.

———. 2013."US Sponsored Stories Facebook settlement triggers Terms of Service changes for global users." www.internetjurisdiction.net/observatory/retrospect/2013-august/.

———. 2014a. "Hong Kong DPA wants to extend European de-index right on Google to Asia-Pacific region." www.internetjurisdiction.net/observatory/retrospect/2014-june/.

———. 2014b. "Marco Civil puts Brazilian data stored abroad under Brazilian jurisdiction." www.internetjurisdiction.net/observatory/retrospect/2014-april/.

———. 2014c. "Twitter blocked in Turkish jurisdiction at IP level." www.internetjurisdiction.net/observatory/retrospect/2014-march/.

———. 2015a. "Microsoft appeals US court order to hand over data stored in Ireland to US law enforcement." www.internetjurisdiction.net/observatory/retrospect/2015-september/.

———. 2015b. "New privacy standards: EU agrees on final draft of its data protection reform." www.internetjurisdiction.net/observatory/retrospect/2015-december/.

———. 2015c. "Belgium asserts jurisdiction over Yahoo, refuses MLAT procedure." www.internetjurisdiction.net/observatory/retrospect/2015-december/.

———. 2015d. "Brazil blocks WhatsApp for 12 hours with accidental impacts in Venezuela and Chile." www.internetjurisdiction.net/observatory/retrospect/2015-december/.

———. 2015e. "French DPA rejects Google's appeal on global application of "right to be de-indexed." www.internetjurisdiction.net/observatory/retrospect/2015-september/.

———. 2015f. "EU DPAs meet with Google, Microsoft, Yahoo to discuss 'right to be de-indexed.'" www.internetjurisdiction.net/observatory/retrospect/2014-july/.

———. 2015g. "Constitutional Court of Colombia rules on "right to be de-indexed" case." www.internetjurisdiction.net/observatory/retrospect/2015-july/.

———. 2015h. "Russian data-localization law might be delayed, some firms could be exempted." www.internetjurisdiction.net/observatory/retrospect/2015-july/.

———. 2016. "UK Home Office reaffirms the extraterritorial reach of the Draft Investigatory Powers Bill." www.internetjurisdiction.net/observatory/retrospect/2016-january/.

Internet Society. n.d. The Internet and the Public Switched Telephone Network. www.internetsociety.org/sites/default/files/The%20Internet%20and%20the%20Public%20Switched%20Telephone%20Network.pdf.

Kleinwächter, Wolfgang. 2001. "Global Governance in the Information Age." Papers from the Centre for Internet Research. http://cfi.au.dk/fileadmin/www.cfi.au.dk/publikationer/cfis_skriftserie/003_kleinwachter.pdf.

Knill, C and D. Lehmkuhl. 2002. "Private Actors and the State: Internationalization and Changing Patterns of Governance." *Governance* 15 (1): 41.

Kuhn, T. 1962. *The Structure of Scientific Revolutions.* Chicago, IL: University of Chicago Press.

McCullagh, Declan. 2010. "State Dept. presses China ambassador on Google." CNET, January 22. www.cnet.com/news/state-dept-presses-china-ambassador-on-google/.

Microsoft. 2015. Microsoft Transparency Hub. Law Enforcement Requests Report January — June 2015. https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/lerr/.

NETmundial. 2014. "Roadmap Section IV: Jurisdiction Issues and How They Relate to Internet Governance." In *NETmundial Multistakeholder Statement.* http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

NETmundial Initiative. n.d. "Terms of Reference." www.netmundial.org/terms-reference.

Nye, Joseph S., Jr. 2014. *The Regime Complex for Managing Global Cyber Activities.* Global Commission on Internet Governance Paper Series No. 1. Waterloo, ON: CIGI.

Ostrom, E. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge, UK: Cambridge University Press.

Palfrey, John and Urs Gasser. 2012. *Interop: The Promise and Perils of Highly Interconnected Systems*. New York, NY: Basic Books.

Raymond, M. and L. DeNardis. 2015. "Multistakeholderism: Anatomy of an Inchoate Global Institution." *International Theory* 7 (3): 572–616.

Scassa, Teresa and Robert J. Currie. 2010. "New First Principles: Assessing the Internet's Challenges to Jurisdiction." *Georgetown Journal of International Law* 42 (4): 1018.

Twitter. 2015. Twitter Transparency Report. Information reuqests January — June 2015. https://transparency.twitter.com/information-requests/22015/jan-jun.

UNESCO. 2013. "Internet Universality: A Means Towards Building Knowledge Societies and the Post-2015 Sustainable Development Agenda." UNESCO Discussion Paper. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/internet_universality_en.pdf.

UN Human Rights Office of the High Commissioner. 2011. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue.* www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf.

———. 2015. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

UN Human Rights Council. 2014. *Resolution A/HRC/26/L.24 on the Promotion, Protection and Enjoyment of Human Rights on the Internet*. http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G14/059/67/PDF/G1405967.pdf?OpenElement.

Weber, Rolf H. 2014. *Legal Interoperability as a Tool for Combatting Fragmentation.* Global Commission on Internet Governance Paper Series No. 4. Waterloo, ON: CIGI.

WSIS. 2005. "Tunis Agenda for the Information Society." WSIS-05/TUNIS/DOC/6(Rev. 1)-E, November 18. https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

Yahoo. 2015. Yahoo Transparency Report. Government data requests January — June 2015. https://transparency.yahoo.com/government-data-requests/index.htm.

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

Executive

President	Rohinton P. Medhora
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Chief of Staff and General Counsel	Aaron Shull

Publications

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Publications Editor	Kristen Scott Ndiaye
Publications Editor	Lynn Schellenberg
Graphic Designer	Sara Moore
Graphic Designer	Melodie Wakefield

Communications

For media enquiries, please contact communications@cigionline.org.

CIGI
67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs
10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org