New World Borders: How Governments Assert Authority Across Borders in the Internet Age

Although the transfer of data across jurisdictions is a fundamental byproduct of the global, interoperable Internet, it can also put pressures on legal systems designed for the pre-Internet age.

On 18 September, GNI co-hosted our 2018 Learning Forum in Washington, D.C., ***"New World Borders: How Jurisdiction Affects Human Rights Online,"*** with the American Society of International Law and the Open Technology Institute at New America. The event brought together human rights and technology policy experts, including GNI members, to explore how governments are responding to these jurisdictional challenges and the corresponding risks for freedom of expression and privacy online.

The event featured sessions focused on two-interrelated forms of state action that affect data flows and human rights: cross-border sharing of electronic evidence, and global content takedown orders.

Session One: Cross-Border Access to Data

Government efforts to access data located in another jurisdiction for law enforcement purposes primarily rely on government-to-government mechanisms. Perceptions that these avenues are too slow and/or cumbersome have spurred various efforts to expedite access by allowing governments to make requests directly to the companies holding this data. The first session explored the legal and historical context of the existing Mutual Legal Assistance Treaty (MLAT) system, as well as its benefits and limitations, and compared the scope and implications of the emerging regimes that would allow for more direct forms of government access to cross-border data.

Professor Jen Daskal began by outlining current alternatives to the MLAT regime, starting with the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act. Signed into law in March of this year,[i] it allows U.S. authorities to compel communications providers to share electronic evidence stored outside the country, with few exceptions. It also permits the U.S. government to execute bilateral executive agreements with partner countries that meet certain rule of law and human rights criteria, thereby allowing designated authorities in those countries to directly request electronic evidence from U.S. providers.

Notwithstanding the human rights criteria set out in the CLOUD Act, *Gregory Nojeim of the Center for Democracy and Technology (CDT)* expressed concern about a "race to the bottom" that could result if countries only meet the minimum requirements necessary to qualify for a bilateral agreement, making it difficult to justify moving away from the MLAT system.

Moving outside the United States, Professor Daskal described a proposed e-Evidence legislation currently being considered by the European Parliament.[ii] This proposal would allow member states to issue orders directly to communications providers. In addition, she highlighted the negotiations underway for an additional protocol to the Budapest Convention on Cybercrime, which may also allow for production orders to be made upon providers, as well as provisions to streamline the MLAT process.

While requests made through MLATs are vetted by the receiving government, to ensure consistency with their domestic law before they are passed along to providers, these new, proposed arrangements would remove that safeguard, potentially leaving companies alone to assess whether requests are consistent with the requesting government's laws and procedures. *Sidsela Nyebak of Telenor* noted that this change may slow down companies' review of incoming requests, which otherwise is generally quite quick. She also pointed out that expectations that companies will thoroughly review requests for legality and against human rights standards may be in tension with corresponding demands for speedy processing established in some of these new proposals. Similarly, Nojeim later expressed concerns that time limits for responding to requests mandated in the e-Evidence proposals will weaken rights protections.

Panelists then walked through how these various mechanisms may relate to one another in practice. Daskal noted that the CLOUD Act's reference to "countries" likely means the U.S. government could not negotiate an executive agreement with the European Union as a block, suggesting instead that a framework agreement may be a good solution. In response, Nojeim expressed concern about the varying standards of justice and rule-of-law within the EU. Professor Daskal also pointed out some differences in how the e-Evidence proposal approaches conflicts of law scenarios in contrast with the CLOUD Act.

Ultimately, panelists agreed that debates on cross-border data flows will continue, and that it is a critical time to engage and shape the norms and laws that emerge, especially the yet-to-be-finalized e-Evidence proposal and the Budapest Convention protocol. Furthermore, the provision of the CLOUD Act requiring the U.S. government to take into account expert input with respect to any executive agreement that is put forward provides a space for non-governmental stakeholders to influence the implementation of that Act.

Session Two: Global Takedown Orders

In recent years, regulators and courts in several different countries have attempted to compel Internet companies to limit the availability of content on their platforms to users in other countries or regions – even where the content at issue has not been deemed illegal and may be protected in those places. These decisions, which push the bounds of extraterritoriality in the exercise of jurisdiction by national authorities, have surfaced with respect to a variety of different categories of content. The second panel

explored the legal and human rights principles implicated by such orders, the reasons why authorities have sought them, and the implications they create for companies and users.

Moderator *Arturo Carrillo of George Washington University Law School* started by outlining two different approaches to the global takedown debate: a "universalist" camp, calling for global enforcement of takedowns, and a "territorialist" camp, calling for strictly local enforcement. Part of the challenge, he noted, results from the fact that while international law standards govern how States prescribe legal norms within their borders, they provide less clarity with respect to how those norms are enforced across borders.

Anupam Chander of Georgetown University Law Center described a number of court cases where these debates are playing out today. Two have been escalated to the European Court of Justice: Google has appealed a ruling by the French Data Protection Authority, CNIL, that an order to delist search results should apply globally (the European Commission recently sided with Google); and Facebook has pushed back on an Austrian order to take down globally a post ruled as hate speech under Austrian law. Google is also litigating against an order issued by the Canadian Supreme Court compelling them to globally delist search results related to an alleged trade secret violation.

Given these challenging conflict-of-law scenarios, *Mark MacCarthy of the Software & Information Industry Association* emphasized the need to focus more on principles that can contribute to consistent applications of laws. He emphasized that while companies cannot be expected to ignore local laws, they also should not be expected to simply remove content globally because a local court said so.

Emma Llanso at CDT further elaborated on the complexity of these decisions. In practice, determined users can get around local content blocking of geographically-registered Internet Protocol (IP) addresses ("geo-blocking"). Meanwhile, alternatives like network disruptions or ISP filtering raise significant freedom of expression and privacy concerns. These jurisdictional debates also complicate the ability of companies to provide users notice when their content is blocked, as well as the ability of users to identify appropriate forms of remedy.
Jessica Dheere of SMEX reminded the audience that for many in the Global South, the approaches taken to content by U.S. and European ICT companies can come across as an extraterritorial application of foreign norms. She also pointed out that, in some cases, content removal decisions are applied regionally, citing examples where companies applied content removals made under the laws of one country to an entire region or language group. She stressed the need to shift the focus of these conversations beyond narrow legal concepts and include the broader idea of justice, and empower users' roles in shaping norms online.

Prof. Carrillo then asked two further questions: First, as we strive for a common standard on content and jurisdiction, can human rights principles be the benchmark? Second, what does good transparency from companies look like in this area?

Prof. Chander and Ms. Llanso noted that human rights principles are an important foundation, but that they may not solve some of the granular speech debates or content moderation questions around issues like hate speech and copyright. Mr. MacCarthy noted that in this vacuum, we are increasingly reliant on companies terms of service as a standard, while Ms. Dheere pointed to UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye's recommendation to link those very terms of service to international human rights standards. On transparency, Ms. Llanso praised the companies' reporting on government requests, but called for greater emphasis on content moderation decisions made pursuant to terms of service.

New Challenges, Same Principles

To close the event, GNI's Director of Learning and Development David Sullivan shared some key takeaways from the day's conversations.

He emphasized that the U.S.-led legal regime has likely contributed to a free and open Internet, the forum highlighted some of the newfound pressures this system is facing, which cannot always be answered by international law principles. He stressed the importance of keeping these jurisdictional issues at the forefront of global technology policy debates, engaging with new actors along the way. Finally, he reminded participants of the critical importance of loudly affirming support for freedom of expression and privacy around the world.

---

[i] GNI experts shared international perspectives on the U.S. CLOUD Act on a session on Capitol Hill: https://globalnetworkinitiative.org/international-perspectives-cloud-act/

[ii] GNI provided written input to the European Commission on the draft e-Evidence legislation: https://globalnetworkinitiative.org/feedback-ec-proposal-e-evidence/