IGF Discussion Preview: A Internet Neutrality Model Framework

by Andrew McDiarmid [1]
October 21, 2013

Among the meetings on CDT's agenda [2] this week at the Internet Governance Forum in Bali is the first meeting of the Dynamic Coalition on Net Neutrality [3]. CDT is a member of the Dynamic Coalition [4], and we contributed a position paper [5] to the group's first annual report, laying out the human-rights arguments for preserving the neutrality of the Internet by law. The report is being published in connection with the inaugural meeting of the group on October 25.

CDT's paper outlines our longstanding position on the Internet neutrality issue in terms of international human rights law. We explain how discriminatory treatment of Internet traffic by access providers threatens users' ability to seek, receive, and impart information of their own choosing, and the ability of entrepreneurs around the world to launch new services that in turn can advance human rights. We also provide principles to guide the enactment of Internet neutrality rules to ensure those abilities and rights are protected.

Model Framework on Internet Neutrality

The coalition's other major output in preparation for the Bali meeting has been a model framework for protecting Internet neutrality [6]. The framework was a collaborative effort among members of the coalition, and as such bears the marks of such a process. There are a few things we would quibble with or state differently, but in general the framework puts forward a strong starting point for what Internet neutrality policy should look like.

The framework gets several key points right. First, it sets a baseline expectation of non-discrimination: providers of Internet access should not favor or disfavor Internet traffic on the basis of its source, destination, content, or associated application. This principle, prohibiting both slowing down and prioritizing traffic, must be the foundation of any approach. In comparison, CDT has concerns with the recent European Commission proposal [7], which calls out blocking and degradation, but leaves some ambiguity around whether prioritization of certain traffic would be prohibited. Allowing ISPs to establish pay-for-priority schemes within their Internet-access offerings would be a substantial loophole that would undermine the basic purpose of establishing Internet neutrality in the first place.

Additionally, the framework appropriately focuses on the provision of Internet access, making it clear that specialized services do not need to be subject to a neutrality obligation, provided they are not offered to the detriment of Internet access. (The fact that the baseline principle is stated in the passive voice – "Internet traffic shall be treated equally" – could invite some ambiguity over who exactly ought to be subject to the rule, but point 2 places the focus squarely and solely on providers of Internet access.) The definition of "specialized services" is not a model of precision, but the idea is right. Internet neutrality rules don't need to unreasonably limit the additional services ISPs can offer; they just need to set some parameters for the Internet access side of the business.

A Few Concerns

Now for the quibbles. First, an omission: like many proposals over the years, the framework seems centered on the possibility of technical discrimination — literally speeding or slowing delivery of certain traffic. It does not specifically confront the possibility of discrimination by pricing arrangements. What if an Internet access provider assesses extra fees on subscribers who choose to use certain online services? What if it favors particular online services by exempting their traffic from a user's capped data allowance, while the use of competing services counts against the cap? It seems increasingly likely that these kinds of scenarios, rather than outright blocking or throttling, will be the future neutrality flashpoints, particularly in the mobile space. The use of "or otherwise

interfering" in point 2 of the framework suggests that such pricing discrimination might be covered under the framework, but the point is debatable, and the framework would be stronger if the issue were confronted directly.

In a few places, the framework strays into issues that either aren't workable or don't seem to belong in an Internet neutrality rule. It contains a provision stating that Internet users have a right to a globally unique IP address (point 5). While this is a laudable goal, the fact is that as IPv4 addresses have become increasingly scarce, some carriers have had to deploy large-scale network-address translation (LSN or carrier-grade NAT, which allows multiple customers share a single public IP address) to keep all their customers connected. The use of LSN raises some concerns [8], but it may be necessary while the transition to the larger address space of IPv6 is ongoing. Unique addresses for every user may be a worthy long-term goal, but given the realities of the transition to IPv6, carrier-grade NAT shouldn't be banned by Internet neutrality rules.

The framework also includes a provision requiring that all traffic inspection examine only headers by default and be done in accordance with data protection requirements. CDT supports strong protections for individual privacy, and ISPs in any given country should be bound by the applicable privacy laws. Also, it's true that neutrality rules tend to have a positive impact on privacy, because barring discrimination reduces ISPs' incentives to examine the content of user traffic. Still, a direct privacy provision seems out of place in an Internet neutrality law. The issues are substantively distinct; neutrality rules aren't directly about protecting user's privacy interests. Protecting Internet users' privacy should be accomplished in separate legislation, not squeezed into an Internet neutrality rule.

Lastly, among its list of network-management exceptions to the neutrality principle, the framework includes efforts to mitigate spam, provided the user has given consent (point 2c). While we understand the philosophical motivation for such a provision, in practice, spam is a significant enough problem that some mitigation practices may be reasonable even if they are employed without specific user consent. User consent is a good practice, but network operators may require more flexibility in their anti-spam strategies.

These issues notwithstanding, CDT welcomes the framework as a strong starting point for governments considering how best to protect Internet neutrality. We also hope that the Dynamic Coalition can serve an ongoing role as a useful venue for discussing and organizing around Internet neutrality policy with advocates and technical experts from around the world. My colleagues Emma Llanso and Matthew Shears are looking forward to representing CDT at the inaugural meeting, and we'll all be engaged in the future work of the Dynamic Coalition.

Source URL:
https://cdt.org/blogs/andrew-mcdiarmid/2110igf-discussion-preview-internet-neutrality-model-framework

Links:
[1] https://cdt.org/personnel/andrew-mcdiarmid
[2] http://cdt.org/igf2013
[3] http://networkneutrality.info
[4] http://www.intgovforum.org/cms/dynamiccoalitions
[5] https://www.cdt.org/files/pdfs/internet-neutrality-human-rights.pdf
[6] http://networkneutrality.info/sources.html
[7] https://www.cdt.org/pr_statement/cdt-welcomes-european-commission-proposal-net-neutrality-calls-closing-key-loophole
[8] https://www.cdt.org/blogs/alissa-cooper/0603paving-way-internet%E2%80%99s-massive-address-switch