KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS ON THE ITU WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS 2012

November 2, 2012

This December, the International Telecommunication Union (ITU) will be amending its telecommunications treaty, the International Telecommunication Regulations (ITRs). While the ITRs have played an important role in promoting interoperability and interconnection of traditional telecommunications systems, a number of the proposed revisions would expand the ITRs to include issues of Internet policy, a shift that could threaten Internet openness, the technical functioning of the Internet, and the exercise of human rights online. CDT has provided the following comments to the Public Views and Opinions page of the ITU website outlining our concerns about the ITU process and about proposed revisions to the ITRs that could threaten the interests described above.
…
…

I. Introduction

We appreciate the opportunity to comment on proposed changes to the International Telecommunication Regulations (ITRs), to be determined at the upcoming World Conference on International Telecommunications (WCIT). In this document, we summarize our overarching concerns about the WCIT process and potential ramifications of extending ITU authority to certain areas of Internet policy-making. We also comment on proposed treaty revisions that we believe could interfere with the civic and economic benefits that the Internet currently brings to societies around the globe.

The ITRs are principle-level regulatory tools that have succeeded in facilitating the growth and impact of telecommunications worldwide. We believe that revisions to the ITRs should seek to strengthen the current communications environment, promoting greater access to and use of communications technologies, but we fear that certain proposed revisions might do the opposite. Below, we describe how ITR revisions that have been proposed in the WCIT preparatory process could threaten the exercise of key human rights online—privacy, access to information, and free expression—and alter Internet functionality in ways that could diminish its civic and economic potential for users around worldwide. Proposals that would so fundamentally change the way the Internet operates are clearly contrary to the original purpose of the ITRs.

CDT believes that the ITRs should remain generalized and not technology-specific in nature. Proposals to include more specific and prescriptive provisions in the ITRs raise significant policy questions that must be carefully deliberated in a multistakeholder process wherein technical, legal, and economic experts have

a meaningful role in decision-making. *Unfortunately, the WCIT process does not follow this model: it is not transparent to the public and it does not offer equitable opportunities for participation to non-state actors. While corporate and civil society entities may purchase Sector membership (if they can afford the high membership fee, an insurmountable hurdle for most civil society organizations), only governments are allowed full participation in the WCIT process. While we appreciate the opportunity to comment, we reiterate that the WCIT is not, and has not been designed to be, a multistakeholder process.*

Below, we outline our concerns regarding specific proposed changes to the ITRs. These are organized by Article.

II. Articles 1 & 2: Scope and Definitions

A number of proposed revisions pending before the ITU seek to widen the scope of the ITRs through changing the definitions of its key terms. One approach is to redefine "telecommunication" by adding either "data processing" or "ICT(s)" - both of which could broaden the ITRs well beyond traditional telecommunications, sweeping in Internet services and applications that deal with user data and content. A second approach is to change the definition of "recognized operating agencies" (currently licensed telecommunications operators) to "operating agencies" so as to subject Internet content and service providers (among many others) to the provisions of the ITRs. Both approaches would represent an enormous expansion of the scope of the treaty, going well beyond the basic technical functions and interoperability of international telecommunications networks and moving into areas of policy-making that require deep expertise on national security, economics, and human rights—issue areas that unquestionably fall outside of the traditional mandate of the ITU.

In the sections that follow, we illustrate the complex policy challenges that would arise if the ITRs were to become applicable to Internet applications, content and service providers.

III. Articles 3 & 4: International Network and Telecommunications Services

A number of proposals seek to impose restrictions on the routing of Internet communications, a change that would allow Member States to collect subscriber identity information in efforts to combat cybercrime. Such control is contrary to the way the Internet works and would require significant re-engineering of the network that could lead to a host of vulnerabilities for users and companies.

A. IP Routing

One proposal would allow Member States to know how online traffic is routed. In the context of international telephony, this makes some technical sense: in simplified terms, telephone communications are conducted over circuit-switched networks, which establish a dedicated link or circuit between the two endpoints of a call. This makes it at least technically feasible to know, and control, the route that an entire communication takes.

However, Internet protocol (IP) networks transmit communications and interconnect entirely differently than traditional telephone networks. When a communication is sent over an IP network, it is broken up into packets, each of which could potentially take a different path across a series of interconnected networks as it journeys to the recipient. A single packet could potentially route through networks hosted in a number of countries before landing at the recipient's computer, all without the control or even knowledge of the sender or recipient. If applied to all Internet communications, the requirement that countries be able to trace the route of every IP packet between its origin and destination would necessitate extensive network engineering changes, not only creating huge new costs, but also threatening the performance benefits and network efficiency of the current system.

User rights to privacy and freedom of expression on the Internet clearly would be threatened by such a policy. While governments may set out to impose these restrictions in order to combat cybercrime, such a policy could give Member States additional technical tools with which they could block traffic to and from certain websites or nations, track citizens' activities online, and block specific individuals from sending or receiving certain communications–all in the name of national security. Furthermore, such re-engineering also would leave government communications' and online activity more vulnerable to interference by bad actors.

B. Quality of Service

Proposals to establish a two-tiered Internet by mandating end-to-end Quality of Service capabilities in addition to a second tier of "best effort" delivery of traffic are also concerning. This model would require network operators to adopt a "pay for priority" model under which content creators could pay higher fees for their content to be carried through the network with a guaranteed "quality of service" that would supersede the lower-tier "best effort" delivery system.

Such a change would stifle innovation by increasing barriers to entry into online content markets and likely inhibit growth in the "best efforts" tier (largely the Internet of today), as operators would turn their focus to more lucrative, higher added-value Quality of Service-based traffic. This would limit incentives for small companies and individuals to enter the online marketplace, likely generating a decline in the potential for economic growth benefits rendered by the Internet as it currently operates.

This model also would undermine the principle of Internet neutrality supported by many stakeholders—it would directly conflict with legislation that protects Internet neutrality in Chile, Finland, and the Netherlands. This principle not only serves to protect the robust economic potential that the current Internet system supports, but also to protect and promote citizens' rights of access to information, which are enshrined by the Universal Declaration of Human Rights.

C. Over-the-Top (OTT) Charging and "Sender Pays" Models

Proposals to impose a "sender-pays" interconnection model on the Internet would replace the current practice of largely settlement-free peering (where different network operators exchange traffic across the global Internet without exchanging payments). Such a change would increase

the role of governments in regulating international interconnection, a significant departure from the lightweight and functional peering system that has supported widespread interconnection among networks.

It would also upend the fundamental operating principles and nature of the Internet, likely to the detriment of all users, whether individuals, business, governments, or others; indeed, only large (and/or incumbent) telecommunications operators would benefit under such a system. Imposing a charging system for traffic, where there currently is none, would penalize those who provide the services, content, and applications that drive Internet traffic, and increase costs to all Internet users (including governments), content and services providers, and others.

This model also could lead to greater restrictions on access to the Internet, mitigating and inhibiting Internet deployment around the globe due to the increased costs both to users and over-the-top content, service, and application providers. Networks could decide not to route traffic through countries if they believed they were not big or commercially important enough to justify the additional cost. This policy could leave users in certain countries on the wrong side of a widening "digital divide," as it would become difficult for them to access important content outside their borders. As this policy would increase costs for networks, they would likely transfer this cost to content creators and to users. This could leave entrepreneurs and other content providers in less developed countries facing greater costs in accessing global markets online. It would also make it difficult for users anywhere to access content in countries where content creators could not afford the cost of sending their content over networks throughout the world.

The proposal has been framed as a policy that will allow telecommunications companies to make greater investments in Internet infrastructure and increasing ICT access, but there is no guarantee that additional revenues would be put towards such development. Instead, the policy could undermine the economic development potential of the Internet, particularly for businesses and independent vendors in developing countries.

D. Voluntary Standards

Proposals to make all (or a selection) of the ITU-T Recommendations mandatory would threaten the growth and stability of the network, interfere with the Internet's economic vitality, and jeopardize openness and free expression online. Such a shift would upend the existing process of technological development on the Internet: those with the most intimate knowledge of technology would be cut out of the technological decision-making process and replaced by government officials who do not write software, run networks, or build computers.

Adoption of technical standards on the Internet has always been voluntary, allowing technology developers to decide how to package and build on standards within their products and services. This tradition has created the most dynamic, innovative communications medium the world has ever seen; it is arguably what sets the Internet apart from previous platforms. Voluntary standards adoption is an important underpinning of that innovation because standards provide the building blocks of Internet technologies – not the technologies themselves. Technology designers are free to piece the building blocks together as they desire to create the hardware, software, and services that Internet users purchase or use.

The mandatory imposition of ITU-T Recommendations would diminish developers' ability to

innovate and likely lock developers into a vision of the Internet as it exists at a particular point in time. Since governments would be loath to constantly add new mandatory requirements to their countries' entire technology sectors, technology companies across the board would be wedded to outdated standards even when some of them would have otherwise been prepared to make upgrades.

The mandatory imposition of any specific set of standards would be problematic, but requiring support for ITU-T Recommendations in particular has additional drawbacks. ITU-T Recommendations comprise just a small fraction of all the standards in use on the Internet today and do not include most of the core standards necessary for global interoperability.

Making ITU-T Recommendations mandatory, while all other standards remain voluntary, would skew technology development in favor of whatever is standardized at the ITU-T, regardless of the technical merit or necessity of ITU-T Recommendations. The result would be a distorted marketplace in which government interests, rather than engineering quality and market technology users' needs, determine how technology companies design their products.

IV. Article 5: Security

CDT recognizes the importance of cybersecurity and the legitimate imperative of expanding both international cooperation and national responses to cybersecurity threats. However, proposals to encourage cooperation among the Member States to combat cybercrime and to harmonize laws on data retention and on the investigation and prosecution of cybercrime raise a host of challenges relating to national security and human rights that we believe do not fall under the purview of the ITU.

While greater cooperation on cybercrime is surely desirable, the ITU has little expertise in these issues—indeed, the word "security" does not appear in the current ITRs. The risk of negative consequences is compounded by the breadth of terms the proposals use in reference to security, from cyberattacks to online crime to protection of information and personal data – concepts that clearly go beyond telecommunications and reach into areas of national security and human rights. Here are two examples of concerns raised by specific proposals:

A. International Cooperation on Security

One proposed amendment to the ITRs would require Member States to cooperate with one another to address issues relating to "Confidence and Security in the provision of international telecommunications/ICT Services." Such a change could make the ITU a primary locus for international cooperation in an area raising many concerns for law enforcement and national security as well as for innovation, privacy, and free expression—none of which traditionally fall under the agency's mandate.

If the ITRs were to address cybercrime at a high level of generality, there also is the risk that some Member States would cite the ITRs a pretext for intrusive or repressive measures. A provision in the ITRs referring to a need for greater information about user activity in the interest of security might be used to support laws that stifle dissent or infringe on privacy. To really

address the issue in its complexity, the ITU would have to address not only the question of how to define cybercrimes without infringing on free expression, but also how to investigate them while respecting the right to privacy.

B. Harmonization of Data Retention Laws

Another proposal urges that Member States cooperate to harmonize their laws on data retention (the requirement that communications companies retain for the benefit of the government data about customers and communications that is not required for business purposes.) This is easier said than done: not only do national laws on data retention vary greatly, but there is ongoing controversy about whether governments should impose data retention mandates at all. And where data retention is required, there are many different views on the legal standards under which governments should be able to gain access to retained data – whether access should require a court order, for example. Such questions are crucial to adopting a data retention law, but are far outside the expertise of the ITU.

Other concerns arise from the fact that data retained by a service provider may, absent specific legal and procedural safeguards, be subject to access by the government to investigate any crime, may be accessed by intelligence agencies, and may be shared with other governments to assist their investigations. In addition, the more data that companies are required to retain, and the longer the retention period, the greater the risk that personal information could be breached, leaked, or otherwise abused.

CDT believes that security is a unique and complex area of policy-making that should not be undertaken without the legitimate involvement of technical, legal, and human rights experts. Making cybersecurity a part of the ITU's treaty also would distract from the efforts already underway by other international bodies more capable of addressing cybersecurity concerns and developing security standards, including such governmental efforts as the Council of Europe Convention on Cybercrime (Budapest Convention), non-governmental, voluntary standards bodies such as the Internet Engineering Task Force, and specialized multistakeholder coalitions like the Conficker Working Group. Finally, given the rapid pace at which cybersecurity threats evolve, and because much of the Internet's critical infrastructure is privately owned and operated, treaty-based bodies such as the ITU are not the ideal source of technical solutions.

V. Conclusion

CDT appreciates the role the ITU plays in supporting the expansion and development of telecommunications networks around the globe. To date, the ITRs have succeeded in facilitating the growth and impact of telecommunications worldwide. However, many of the proposed revisions to the ITRs will now do exactly the opposite. Through extending the regulatory framework of the ITRs to the Internet, the ITU Member States will mitigate the Internet's growth and inhibit the Internet's impact on economies and societies around the globe.

As an organization dedicated to protecting and promoting the civic and economic benefits of the Internet, we urge Member States to ensure that the ITRs continue to allow the communications environment to flourish and promote greater access to and use of communications technologies

by citizens throughout the world. Member States should reject proposals that could increase the costs of Internet use, stifle technological innovation, and/or threaten the exercise of human rights online.

We would like to thank the ITU Secretariat for the opportunity to provide these comments in a public setting.

The Center for Democracy & Technology (CDT) is a US-based non-profit civil society organization working to keep the Internet open, innovative, and free. With expertise in law, technology, and policy, CDT is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

For more information, contact Ellery Biddle, Policy Analyst (ellery@cdt.org) or Emma Llansó, Policy Counsel (ellanso@cdt.org).