CENTER FOR DEMOCRACY & TECHNOLOGY

Comments of the Center for Democracy & Technology
On Freedom of Expression and the Telecommunications and Internet Access Sector

1 November 2016

The Center for Democracy & Technology welcomes the opportunity to provide input for the report that the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression, David Kaye, is preparing on the role of telecommunications and Internet access providers in freedom of expression. Below, we provide information and resources that pertain to three areas of inquiry of this study:

In response to the examination of policies and practices that affect users' access to information and governments' access to user data, we include an overview of our recent papers on zero-rating practices and systematic government access to private-sector data.

Concerning trends in state regulation that involve content censorship/filtering or access to user data, we include our comments to the United States Department of Justice on cross-border law enforcement demands.

Regarding the role of relevant standards bodies in protecting freedom of expression, we include a draft informational document for Internet engineers that provides an overview of technical censorship techniques. (This document is an Internet draft currently under consideration by the Internet Engineering Task Force.).

I. Practices and Policies of Telcos and Its Impact on the Right to Free Expression

A. Zero Rating: A Framework for Assessing Benefits and Harms

Zero rating – the practice in which a telecommunications provider sets a data cap for its subscribers and counts some, but not all, of the subscriber's Internet usage toward that cap – has proved controversial. Many advocates have voiced concerns that zero rating could inhibit diversity of expression and access to information, due to the provider's preferential treatment of some content providers over others. Others, however, have argued that zero rating could play a valuable role in making Internet access more affordable to a broader range of people, in both developing and developed economies. CDT advocates for the power of the open Internet as an engine of free expression and economic development in our recent paper "Zero Rating: A Framework for Assessing Benefits and Harms."[1]

[1] Erik Stallman & R. Stanley Adams, Zero Rating: A Framework for Assessing Benefits and Harms (Jan. 13, 2016), available at https://cdt.org/files/2016/01/CDT-Zero-Rating_Benefits-Harms5_1.pdf.

The framework we propose advances an alternative perspective in the polarized zero rating debate. We approach zero rating in a manner similar to other key questions in implementing and applying net neutrality laws and regulations, such as network management, usage-based pricing, or specialized services that rely on the same infrastructure as the public Internet while serving a separate function. Answering these types of question often requires a multi-factored and fact-specific approach.

Our framework evaluates zero rating's impact on the open Internet and broadband adoption by looking both to a specific zero-rating arrangement's influence on edge providers and users as well as attributes of the broadband market in which that arrangement is offered. We focus on the importance of users maintaining control of the content and services they access or create via the Internet. Finally, we consider whether zero rating will serve as an on-ramp to full access to the open Internet or as a roundabout of curated offerings that users exit only at great effort and expense. We conclude that this depends on some fundamental and interdependent factors of the broadband market: existing levels of adoption and deployment, competition, and digital literacy and education.

B. Systematic Government Access to Personal Data: A Comparative Analysis

CDT's paper, "Systematic Government Access to Personal Data: A Comparative Analysis," provides detailed information about the laws, regulations, and practices that govern government access to data held by telecommunications and Internet access providers.[2] In recent years, there has been an increase worldwide in government demands for data held by the private sector. This increase includes an expansion in government requests for 'systematic access': direct access by the government to private-sector databases or networks, or government access, whether direct or mediated by the company that maintains the database or network, to large volumes of data. Governments around the world have always demanded that commercial entities disclose data about their customers in connection with criminal investigations, enforcement of regulatory systems, and national security matters. Companies have always felt an obligation—and oftentimes are under legal compulsion—to cooperate, but they have also felt a business need and sense of responsibility to protect their customers' personal data and, in most cases, have diligently sought to balance those interests. This paper is the culmination of research that began in 2011, and included the commissioning of outside experts to write reports about laws, court decisions, and actual practices relating to systematic government access in 13 countries.

Systematic access raises hard questions for companies that face demand for government access to data they hold. They must decide whether the demand or request is lawful, though the law may be vague. Moreover, companies must decide what information about their responses to these demands they may disclose to their customers and to the public. This trend toward systematic collection and lowered standards for trans-border surveillance poses substantial concerns for free expression and human rights. Many of our concerns on this issue focus on the existence and scope of state duties to protect and respect privacy and free expression of people outside the state's territorial boundaries.

[2] Ira S. Rubenstein, Gregory T. Nojeim & Ronald D. *Lee, Systematic Government Access to Personal Data: A Comparative Analysis*, 4 Int'l Data Privacy Law 96 (2014), *available at* https://cdt.org/files/2014/11/government-access-to-data-comparative-analysis.pdf.

While free expression is universally recognized as a human right, some governments assert that this right and its obligation have a territorial limit.

In addition, countries draw different distinctions between content and "non-content"/metadata in their standards for government access, which can raise free expression issues. A number of countries draw a legal distinction between the content of communications and various types of non-content, establishing higher standards for government access to the former and lower standards for access to the latter. For example, Brazilian courts have ruled that "judicial authorization is not required for the Police or the Public Prosecutor's Office to have access to subscriber-identifying data from companies," on the grounds that anonymous speech is constitutionally prohibited. British law imposes very few controls on access to non-content data (both communications attributes and subscriber data), which are easily accessible by a very large number of central and local officials, simply requiring that a senior official make a request. These standards can vary considerably by country, and government access to either type of user data can have a chilling effect on freedom of expression.

II. Cross-Border Law Enforcement Demands

On July 15, the U.S. Department of Justice proposed legislation that would permit foreign governments hand-picked by DOJ to conduct wiretapping in the U.S. for the first time, and to do so without a court order based on probable cause of crime. The legislation would implement a bi-lateral agreement the DOJ has already negotiated with the United Kingdom, the current text of which was not publicly released. Bilateral cross-border law enforcement demands (C-BLED) agreements such as those contemplated in the legislation the DOJ has proposed could be part of the solution if limited to stored content and metadata, and if based on strong human rights standards.

In our analysis of the proposed bill,[3] CDT emphasized that in any such agreement, a finding should be required that the country with which an agreement would be struck does not engage in torture or cruel, inhuman, or degrading treatment or punishment, prohibits arbitrary arrest and detention, provides fair trial rights, freedom of expression, association and peaceful assembly, and protects against the arbitrary and unlawful interference with privacy. Rather than merely "demonstrate respect for the rule of law and principles of non-discrimination" as suggested in the DOJ legislation, we proposed that any legislation to authorize C-BLED agreements should prohibit agreements with countries that show a pattern of discrimination or of conduct inconsistent with the rule of law.

The DOJ bill also would require that orders issued under a C-BLED agreement "may not be used to infringe on freedom of speech," but does not indicate under which country's law "infringement" will be tested. Rather than try to resolve this issue directly, we argue that a better approach would be for C-BLED agreements to adopt the dual criminality requirement that pertains in U.S. law today. We provide our analysis of this bill to highlight many of the issues that will arise as governments attempt to resolve the challenges of cross-border access to communications data.

[3] *Cross-Border Law Enforcement Demands: Analysis of the US Department of Justice's Proposed Bill*, Center for Democracy and Technology (Aug. 17, 2016), *available at* https://cdt.org/files/2016/08/DOJ-Cross-Border-Bill-Insight-FINAL2.pdf.

CENTER FOR DEMOCRACY & TECHNOLOGY

III. Activity in Standards Bodies in Protecting and Promoting Freedom of Expression

Censorship by state or private actors online often seeks to leverage features of the technical architecture of the Internet. CDT's Chief Technologist, Joseph Lorenzo Hall, is developing an informational document within the Internet Engineering Task Force (IETF) that describes the technical mechanisms used by censorship regimes around the world to block or impair Internet traffic.[4] The aim of the document is to raise awareness among engineers to the properties being exploited and mechanisms used to censor end-user access to information.

As a reference to various ways network censorship is achieved, the document describes three elements of Internet censorship: prescription, identification, and interference. Prescription is the process by which censors determine what types of material they should block. Identification is the process by which censors classify specific traffic to be blocked or impaired. For example, under a relatively simple filtering scheme, censors would block or impair access to all websites that contain "sex" in the title or traffic to "sex.com." Interference is the process by which the censor intercedes in communication and prevents access to censored materials by blocking access or impairing the connection.

CDT is developing this informational document within the IETF's RFC ("Request For Comment") system to encourage those who create technical standards to consider the potential implications for censorship of the technologies they design.

* * *

Thank you for the opportunity to contribute to this important report. We look forward to future engagement with the Special Rapporteur on these topics.

Sincerely,

Emma J. Llansó
Taylor Moore

Center for Democracy & Technology

[4] J. Hall et al., *A Survey of Worldwide Censorship Techniques Draft-Hall-Censorship-Tech-04* (July 8, 2016), *available at* https://tools.ietf.org/pdf/draft-hall-censorship-tech-04.pdf.