



ELECTRONIC FRONTIER FOUNDATION

Protecting Rights and Promoting Freedom on the Electronic Frontier

EFF CONTRIBUTION TO THE BRAZILIAN PARLIAMENTARY INQUIRY COMMISSION

CONTACT

Katitza Rodríguez | International Rights Director | katitza@eff.org

Thank you for providing the Electronic Frontier Foundation (EFF) with the opportunity to present our contribution to the discussions of the Brazilian Parliamentary Inquiry Commission on Cybercrimes. EFF is the leading international nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.

Even in the fledgling days of the Internet, EFF understood that protecting access to developing technology was central to advancing human rights for all. In the years that followed, EFF used our independent voice to clear the way for open source software, security research, encryption and a world of emerging technologies. Today, EFF uses the unique expertise of leading technologists, activists, and attorneys in our efforts to defend free expression online, fight illegal surveillance, advocate for users and innovators, and support freedom-enhancing technologies. EFF advises policymakers and educates the press and the public through comprehensive analysis, educational guides, activist workshops, and more. EFF empowers hundreds of thousands of individuals through our Action Center and has become a leading voice in online rights debates.

EFF would like to comment on the following proposals and statements made by the Commission:

BACKGROUND INFORMATION

“[...] it seems important to include in the Marco Civil da Internet an exception to the general rule of network neutrality in order to confirm the Brazilian judiciary possibility to request that

815 Eddy Street • San Francisco, CA 94109 USA

voice +1 415 436 9333

fax +1 415 436 9993

web www.eff.org

email information@eff.org

connection providers adopt technical measures to block traffic, as it already happens in other Western democracies like for example the countries of the European Union, the United States and Chile.”

“As pointed out by the Sub-Rapporteurs Mr Alex Sandro and Rafael Motta, in such cases blocking access to criminal content is the only way to guarantee the effective protection of users in extreme cases in which the applicable alternatives have been exhausted. Therefore, having received fruitful contributions from various organizations and authorities, we propose a bill that allows, in extreme cases, the blockage of Internet applications considered criminal after a court order. This approach has been adopted in many democratic countries. The Chilean legislation, for example, deals with network neutrality in an extremely extensive way, but does not exclude the possibility of blocking websites that provide illegal content or services (Ley 20,453 art. 24H). The Regulation 2120 of 2015 states of the European Parliament and of the Council states in its art. 3 that users have access to content and services, provided they are legal and allowing blockages to comply with the law or court orders. Similarly, in the United States Federal Communications Commission's Resolution Protecting and Promoting the Open Internet, from April 13th 2015, determines that the user has the right to access destinations on the Internet that are legal and that providers may not block lawful content. Thus, websites or content that are considered illegal by the justice are subject to being blocked in many democratic countries.”

Blocking of websites and Internet applications

Proposal to change the Marco Civil da Internet (MCI) so that Internet applications (such as WhatsApp and YouTube) and websites can be blocked after a court order.

Justification: preventing crimes against copyrights and the sharing of criminal content in general.

Proposal: The Commission (CPI) proposes a bill modifying the MCI to allow the blockage of Internet applications by court orders. This would add a 4th paragraph to Article 9 of the MCI stating that: "Once, in the course of the judicial process, the alternatives for punishment predicted by law are exhausted without the cessation of the conduct considered to be

criminal, the judge may oblige connection providers to block access to content or Internet applications related to that conduct taking into account the proportionality, the reach of the measure, the severity of the crime and the speed necessary to provide the effective cessation of such conduct."

ELECTRONIC FRONTIER FOUNDATION CONTRIBUTION

United States legislation does not authorize the blockage of Internet applications such as WhatsApp and YouTube. The United States Federal Communications Commission's resolution Protecting and Promoting the Open Internet was issued within a context of broad, extensive legal protection against liability for Internet service providers which ensures that ISPs are generally not held responsible for the content of the traffic they carry, nor for others' use of their services, regardless of whether those uses are legal or illegal. The Commission's order applied neutrality obligations only to "legal" content. The Open Internet order is completely silent about other matters; it does not in itself purport to authorize or require any content removal or blockage. (Neither do laws like the Digital Millennium Copyright Act anticipate that a provider could be required to block or filter content from the wider Internet, as opposed to removing content that it hosts.) And the Open Internet Order, as with all U.S. law, is constrained by the First Amendment to the Constitution, which prohibits all government authorities from blocking more speech than is necessary to fulfill a compelling government purpose.

A reader of the Open Internet resolution might form the mistaken impression that the United States has a practice of site blocking by Internet service providers. We would like to emphasize that the blocking of Internet services (whether domestic or foreign) is a very rare occurrence in the United States, even in the case of services that facilitate illegal activity, and even pursuant to court order. We are not aware of any example of a valid court order in the United States that required an Internet access provider to make third-party sites or services inaccessible. Such orders would likely be invalid under the First Amendment. As far as we know, the U.S. government has also not suggested that providers have obligations to prevent access to foreign sites, forums, or communications media that exist completely outside of the government's jurisdiction, or due to failure to comply with court orders.

The possibility of creating a legal obligation for Internet service providers to block users' access to third-party sites outside of U.S. jurisdiction was raised in a controversial 2011 bill called the Stop Online Piracy Act (SOPA). SOPA would have authorized court orders directed to Internet service providers to require them to block access. This legislation was widely criticized in the U.S. and its consideration was withdrawn by the Congress in the face of a storm of protest, including significant opposition from technical experts, industry, and ordinary Internet users. SOPA was never enacted into law. The breadth and intensity of opposition to SOPA and its failure to pass underscores the fact that, not only is ISP website blocking not the law in the United States, it remains extraordinarily controversial here.

A law that purported to authorize a court to block an entire Internet application such as WhatsApp could never be proportionate due to its effect on the freedom of expression of large numbers of innocent Internet users. Blocking an entire application will inevitably affect a significant amount of lawful expression. Such blocking also contravenes best practice standards such as the Manila Principles on Intermediary Liability (<https://manilaprinciples.org>) which prescribe that "restriction of content should be limited to the specific content at issue" and that "the least restrictive technical means must be adopted". In the United States, such blocking would contravene the First Amendment and in Brazil it would contravene section 5 of Article IX of the Constitution of Brazil. The United Nations Special Rapporteur on Freedom of Expression and Opinion has stated that:

blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal.

The broad safe harbor that U.S. law afford to Internet platforms under U.S. law has been responsible for those platforms flourishing and extending their reach throughout the world. This is because by relieving them of the responsibility to vet or censor content passing over their networks, they have been enabled to open up those network to a diversity of content and applications. Along with network neutrality, this principle of "permissionless innovation"

has been a key driver of the Internet's explosive growth as a medium for communication and commerce.

Conversely, if the law gives Internet platforms reason to fear that they will be required to monitor and censor what their users do online in order to avoid legal cost and risk, those services will be designed to strictly limit the capacity for users to express themselves freely and to experiment. This in turn will reduce domestic online innovation and drive investment in online platforms overseas. Ultimately, a permissive online content regulation regime is therefore not only good for users, but also good for Internet companies, and for the digital economy at large.

Sincerely,

Jeremy Malcom, Senior Policy Analyst

Katitza Rodríguez, International Rights Director