

Access Now submission to the United Nations Human Rights Council, on the Universal Periodic Review 2016 Cycle for Brazil

About Access Now

1. Access Now (www.accessnow.org) is an international organisation that works to defend and extend digital rights of users globally. Through representation in 10 countries around the world – including presence in Latin America- Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. We engage with an action focused global community, and our Technology Arm operates a 24/7 digital security helpline that provides real time direct technical assistance to users around the world.
2. Access Now advocates an approach to digital security that promotes good security policies that protect users' human rights, including privacy and freedom of expression. Access Now has worked extensively in Latin America on digital rights. We now welcome the opportunity to provide feedback on the Universal Periodic Review 2016 Cycle for Brazil.
3. This is the third review for Brazil, last reviewed in March 2012 where the Brazilian government voluntarily accepted and pledged to implement 170 recommendations in the area of human rights during the review at the Universal Periodic Review (UPR) in Geneva.

Domestic and international human rights obligations

4. Brazil has signed onto various international human rights instruments, including the [Universal Declaration of Human Rights](#) (UDHR), [International Covenant on Civil and Political Rights](#) (ICCPR), the [American Convention on Human Rights](#), the [Convention against Torture](#) (CAT), the [International Covenant on Economic, Social and Cultural Rights](#) (ICESCR), the [International Convention on the Elimination of All Forms of Racial Discrimination](#) (CERD), the [Convention on the Elimination of all Forms of Discrimination Against Women](#) (CEDAW) and the [Convention on the Rights of the Child](#) (CRC) and the [Convention against Enforced Disappearance](#) (ICCPED).
5. The Brazilian Constitution (1988) contains human rights provisions in art. 5º, regarding fundamental rights, and arts. 6º, 7º, 8º, 9º, 10 and 11, that guarantee citizens' social rights. It includes specific guarantees to the rights to freedom of expression (art. 5º, IV, VIII and IX), privacy (art. 5º, X, XI, XII) and access to information (art. 5º, XXXIII).¹
6. Law N° 12.965/2014, The Civil Rights Framework for the Internet (Marco Civil da Internet) commits to international human rights principles through domestic

¹ Constitution of the Federative Republic of Brazil: constitutional text of October 5, 1988, with the alterations introduced by Constitutional Amendments no. 1/1992 through 64/2010 and by Revision Constitutional Amendments no. 1/1994 through 6/1994. – 3. ed. – Brasília: Chamber of Deputies, Documentation and Information Center, 2010.

legislation, by affirming freedom of expression (art. 3º, I) and privacy (art. 3º, II) as core principles for internet use in the country. It also recognizes all citizens' rights to access the internet (art. 4º, I) and to access information, knowledge, and culture, as well as to participate in decisions about public affairs (art. 4º, II).

Situation of digital rights in Brazil

7. Despite these commitments and obligations, we have gathered and hereby submit evidence of a systematic disregard of digital rights in Brazil. These violations include:

Violations of access to information & freedom of expression

8. On May 3, 2016 a judge ordered WhatsApp blocked for 72 hours. The outage lasted for just over 24 hours before a judge reinstated access to the popular messaging application. Soon after, an emergency petition was filed against cybercrime bills in Brazil that would authorize blanket internet shutdowns. In total, lower court judges have ordered three Whatsapp shutdowns in the country in the last two years. The blocking orders are directed to telecommunications companies that will receive daily fines in case of non compliance. Although some of the decisions were kept secret, the latest one -- from July² -- was made public and showed the justification behind it: the company's failure to comply with a court order in a criminal investigation that demanded the "interception" of messages. The demands were for the "suspension of the encryption key" and the deviation in real time of the messages exchanged "before the implementation of the encryption." Although these Brazilian shutdowns have been usually followed by higher courts' decisions overturning them for being disproportionate, they have serious impacts for the exercise of freedom of expression and access to information. Additionally, they evidence an intention from some groups in the government to use these legal mechanisms to push for a weakening of strong encryption systems and for more invasive means to conduct investigations, putting privacy at risk.³
9. As part of the preparations to host the 2016 Rio Olympic Games, the Brazilian telecom authority, ANATEL, granted the Brazilian Armed Forces the ability to use equipment that, in addition to "jamming" illegal drones and potentially thwarting potential terrorist attacks, could shut off all or parts of mobile internet. The permit is partially kept in secret and there is little clarity as to how this technology will be deployed in the future and which are the conditions for its use. Although authorities

² Access Now. July 19th, 2016. "On eve of Olympics, judge orders blocking of WhatsApp in Brazil" <<https://www.accessnow.org/eve-olympics-judge-orders-blocking-whatsapp-brazil/>> accessed in September 19th, 2016.

³ After the last Whatsapp shutdown, the Brazilian Justice Minister, Alexandre de Moraes, has stated that he wants to propose a digital data bill that would, among others, force companies to establish their offices in Brazil. According to a report from The Fortune, "the bill should provide a framework for cooperation with authorities without depriving about 100 million users of the popular Facebook messaging service". See: Fortune. July 20th, 2016. "After Third WhatsApp Shutdown, Brazil Plans to Draft Digital Data Bill". <<http://fortune.com/2016/07/20/third-whatsapp-brazil-shutdown/>> accessed in September 19th, 2016.

claim the permit's purpose is limited to blocking drones, there is not a clear commitment to not using it to shut down mobile internet access.⁴

Additional legal provisions that violate the freedom of expression

10. Contradicting international human rights bodies' recommendations and its own commitments with the protection of freedom of expression, Brazil criminalizes offenses against honor (Penal Code, arts. 138 to 145) and legislators have attempted to increase penalties for offenses committed with the use of the internet. One such legislative proposal is PL 4148/2015 that proposes to change the Penal Code to increase penalties if the offense is committed through the internet or telephone applications. The bill is pending approval by the Chamber of Deputies together with PL215/2015 (see below).
11. A number of proposals try to introduce local interpretations of the “right to be forgotten.” Considering that Brazil has been criticised for the extended use of defamation lawsuits to silence political opposition and critique of public authorities, a large number of concerns have been raised by human rights organisations regarding the implementation of an ill-conceived “right to be forgotten,” which could be abused to alter or erase the public record. Despite this opposition, legislators are avid to develop bills focusing on such a right to “de-list” - there are at least three bills being discussed in the Congress to that end (PL 215/2015; PL 1676/2015; PL 7881/2014) - while little attention has been given to the approval of a data protection act. Data protection legislation is critical to ensuring personal data is protected and citizens are empowered to control how their information is treated online.
12. The protection of copyright has also been cited as a justification for various legislative proposals, including for the introduction of the so-called “notice and stay down” mechanisms and the blocking of internet applications. PL 5203/2016 was a result of the CPICIBER and changes the Marco Civil in order to oblige internet service providers to make unavailable any identical copies of original content considered to be infringing the law by a court order, without the need of additional court orders and in 48 hours (notice and stay down). Additionally, PL 5204/2016 authorizes judges to order the blocking of “internet applications” hosted outside of the country in case they commit crimes punishable with more than two years of incarceration (which includes copyright violations), except crimes against honor. According to the current text, the bill should not be applied against instant messaging applications.
13. With the justification of protecting children's rights, PL 2390/2015 proposes to create a national, mandatory “real name” identification policy to restrict minors' access to supposedly inappropriate content. Mandatory real name policies, which require users to present legal identification to register accounts or access the internet, risk

⁴ Access Now. August 5th, 2016. “Access Now urges Brazil not to jam communications during Olympic games” <<https://www.accessnow.org/access-now-urges-brazil-not-jam-communications-olympic-games/>> accessed in September, 20th 2016.

- thwarting the expression of vulnerable groups such as political and sexual minorities who may choose to withhold their opinions or expression out of fear for reprisals.
14. While the Marco Civil regulatory decree is known for being important legislation affirming digital rights, there are concerns on interpretation and criticism that some articles are too broad in scope, which could negatively impact internet users' rights, particularly on issues such as the ability of judges to order the blocking of applications or services.
 15. Regarding the issue of Net Neutrality in Article 2 of the Marco Civil regulatory decree, “specialized services” are not included within the scope of the article and therefore not included in the regulations detailed in the text and failed to widespread zero rating practices in Brazil. Such omissions leave an open door to dangerous internet traffic prioritization that leads to negative consequences for freedom of expression.

Violations of the right to privacy

16. In August and September 2016, Brazil hosted the Olympic and Paralympic Games. The preparation for them was once again followed by an increase in the country's investment in mass surveillance technologies. Having already hosted several large-scale international events in the past years, Brazil has become a privileged market for international surveillance companies. Among other things, Brazil has (i) significantly increased the number of cameras installed on city streets, (ii) installed several integrated command centers that can track conditions in real time and allow for coordinated responses by different municipal, state, and federal departments, (iii) acquired surveillance balloons equipped with monitoring systems that were originally developed for military use and (iv) monitored social media accounts of participants of protests.⁵
17. Despite the potential abuses to privacy these mass surveillance technologies represent, they were not followed by a proper public debate on their future uses or transparency measures as to their acquisition and use. Besides that, there are serious regulatory gaps regarding the limits and rules in which they will be implemented. For instance, while the use of street surveillance cameras increases each year — and significantly increased during the Olympic games — Brazil lacks proper legislation to regulate how images are protected and safeguarded after they are used.
18. In May 2016, the final report of a Parliamentary Commission of Inquiry on Cybercrimes (CPI-CIBER) created in the Chamber of Deputies to investigate online crimes and their effects in Brazil introduced concerning bills in Congress that may put the protection of the right to privacy at risk. The proposed legislation includes an extension of the existing mandatory data retention obligations to everyone who provides internet access, such as free access points in malls, public transport

⁵ Jamila Venturini and Amie Stepanovich. (Access Now, August 24th, 2016) “Brazil's Olympic surveillance legacy” <<https://www.accessnow.org/brazils-olympic-surveillance-legacy/>> accessed in September 19th, 2016.

stations or airports (PL 3237/2015).⁶ The same bill also states that if the same IP address is shared among different users, internet service providers should retain all the technical information necessary for the individual identification of a user (art. 2°). Despite the broad language adopted and the clear violations to the principles of necessity and proportionality of these measures, the bill was approved in August 2016 by the Science and Technology Commission at the Chamber of Deputies and is now pending discussion in a Constitutional Commission being sent to discussion in the Senate.

19. In October 2015, the Chamber of Deputies' Constitutional Commission approved PL 215/2015, which changes the current version of the Marco Civil regulatory decree to expand an exception that was added to art. 10 conceding that subscriber information such as "personal qualification, affiliation, and address" may be handed over to competent authorities without a court order.⁷ The bill expands the list of items that can be obtained without judicial review to include e-mail address, telephone number and the national security number (CPF) and obliges providers to collect, obtain, organize and make available such information.⁸
20. On May 12th, 2016, the Executive sent a draft data protection bill to the Chamber of Deputies. The bill (PL 5276/2016) is the result of two processes of public consultation led by the Ministry of Justice in 2010 and 2015 that involved academia, civil society organizations and the private sector. Despite being sent with a request to be urgently debated and voted, it is still pending discussion by legislators. Brazil has sectorial legislation on the subject, but it is one of the few countries in the region that does not have a comprehensive data protection framework in place.⁹ The absence of such unified framework has given a wide margin of discretion to private and public agents in dealing with citizens' personal information (see paragraph 13) in a way that contradicts data protection principles and good practices.

Recommendations

⁶ According to Law N° 12.965/2014, Internet Service Providers should retain connection logs -- date and time of the beginning of the internet connection, duration of the connection and IP address -- for the period of one year.

⁷ The provision that authorizes competent authorities to request so-called subscription data without a court order (art. 10, §3o) was added to the text of the Marco Civil da Internet to respond to what was already predicted by a previous law on money laundry (Law N. 12.683/2012). See: Rossini, C; Cruz, F. & Doneda, D. (2015). The Strengths and Weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet. <https://www.cigionline.org/sites/default/files/no19_0.pdf#page=16> accessed in September 19th, 2016.

⁸ Danny O'Brien (EFF, October 14th, 2015) "Brazil's Politicians Aim to Add Mandatory Real Names and a Right to Erase History to the Marco Civil" <<https://www.eff.org/deeplinks/2015/10/brazils-terrible-pl215>> accessed in September 19th, 2016.

⁹ Dahlmann, A.; Venturini, J.; Dickow, M. & Maciel, M. (2015). Privacy and Surveillance in the Digital Age: a comparative study of the Brazilian and German legal frameworks. <https://www.academia.edu/18159512/Privacy_and_Surveillance_in_the_Digital_Age_a_comparative_study_of_the_Brazilian_and_German_legal_frameworks> accessed in September 19th, 2016.

8. Brazil can improve its human rights record and treatment of digital rights in several areas. We accordingly recommend that the government of Brazil:
 - a. Refrain from attempts to weaken the Marco Civil regulatory decree and emphasize the need to protect users rights in the implementation of regulatory legislation.
 - b. Commit to the prompt legislative treatment and approval of the data protection bill that arose from public consultations and the interaction with multiple stakeholders.
 - c. Call attention and propose specific measures to avoid mistaken legal interpretations that enable internet shutdowns and abandon legislative proposals that aim at facilitating this practice
 - d. Reform the Penal Code to eliminate crimes against honor and reject bills trying to increase penalties for offenses committed through the internet.
 - e. Call to guarantee the enjoyment of net neutrality (in light of regulations contained in the Marco Civil).
 - f. Refrain from introducing the right to de-list by law, to avoid abuses by public authorities against the rights to freedom of expression and access to information.
 - g. Refrain from pressuring or forcing internet and communications technology companies to weaken their encryption mechanisms or introduce vulnerabilities.
 - h. Review existing policies on data retention in light of the International Principles on the Application of Human Rights to Communications Surveillance¹⁰ and reject any proposal to extend them.
 - i. Introduce strong and effective transparency and oversight mechanisms to all matters related to mass surveillance and the acquisition of surveillance technology.
9. The UPR is an important U.N. process aimed at addressing human rights issues all across the globe. It is a rare mechanism through which citizens around the world get to work with governments to improve human rights and hold them accountable to international law. Access Now is grateful to make this submission.
10. For additional information, please contact Access Now staff Peter Micek (peter@accessnow.org).

¹⁰ International Principles on the Application of Human Rights to Communications Surveillance. Available at <https://necessaryandproportionate.org/>