INTERNATIONAL ENCRYPTION BRIEF

MARCH 2021

The Encryption Debate in Brazil: 2021 Update

Priscilla Silva, Ana Lara Mangeth, and Christian Perrone

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Introduction

The encryption debate in Brazil, much as in Latin America and the Caribbean and across most of the globe,[1] continues to be framed as a tension between, on the one hand, data and communications security and, on the other hand, accessibility for law enforcement and national security purposes. End-to-end encryption in messaging services is central to this discussion, especially because these services are growing in popularity and now have a more profound impact on investigations and intelligence gathering. Two major cases mentioned in a previous brief[2]—both reviewing the suspension of WhatsApp for not complying with judicial orders requiring the company to hand-over decrypted data—are yet to receive a final decision from the Brazilian Supreme Court. The justices rapporteurs, however, have presented their opinions against the suspension of the messaging service.

New Updates

The coronavirus pandemic brought a number of issues related to cybersecurity, online misinformation, and access to overseas data to the forefront of the tech policy landscape. Trying to address these issues, all three branches of the Brazilian government have directly or indirectly influenced the country's debate on encryption. The focus here is on the role of the judiciary, looking at the WhatsApp cases presented before the Brazilian Supreme Court. These cases are relevant because they are the first time that the Supreme Court has been asked to rule on whether end-to-end encryption is permitted under Brazilian law and if so whether it would not be obligatory to have access opportunities ("backdoors") for law enforcement agencies. The cases have repercussions not only throughout Brazil, but should also draw the attention of the international community because it hinges upon cybersecurity of private communication at large.

The issue of encryption was revisited with the enactment of the General Data Protection Law ("LGPD") in August 2018. The legislation reshaped the debate even before entering into force in September 2020.[3] The justices rapporteurs issued their opinions in June, yet they made express references in their votes to the Federal Constitution, the Internet Bill of Rights,[4] and the LGPD. Thus, data protection was front and center in the justices' views, and it builds upon the history of protecting digital rights brought by the Internet Bill of Rights and its implementing decree,[5] which already articulates, among others, the principles of net neutrality and privacy and different safeguards against mass surveillance. The opinions also encourage the use of technologies that uphold the inviolability of data and the widespread adoption of encryption.

Ongoing Cases: Encryption debate on WhatsApp blocking

End-to-end encryption, particularly on the messaging service WhatsApp, is a challenge for law enforcement and intelligence agencies, since it may preclude lawful access to the content of private communications, directly impacting investigations and the enforcement of personal liability. Between 2015 and 2016, even before the case reached the Supreme Court, regional courts suspended WhatsApp nationwide on three occasions. Court decisions aimed at gaining access to decrypted content hosted by the messaging service to further investigate alleged crimes committed by WhatsApp users in Brazil. The company's explanation that the application's architecture and encryption protocols were incompatible with the different judicial requests of access to decrypted data was deemed insufficient by the courts. This motivated two constitutional challenges that were subsequently brought before the Brazilian Supreme Court to discuss the nationwide suspension of WhatsApp's services, ADI No. 5527 and ADPF No. 403.[6] As of writing, both cases are pending final decisions.

The cases question whether the ban is proportional, given WhatsApp's inability to comply with legal requests to access data without fundamentally redesigning the application's architecture and encryption protocols. The outcome of the cases depends on two questions: Is encryption legal in the first place, and, if so, should companies that provide encrypted services be obligated to create either backdoor or exceptional mechanisms of access? The arguments raised in favor of encryption state that cryptography protects privacy, personal data, and free speech and should be allowed as a matter of freedom of enterprise. In other words, companies, as a matter of principle, should be free to choose their own business models. Critics, on the other hand, argue that law enforcement agencies uphold the fundamental public interest in security, and exceptional mechanisms of access, thus, should be able to request access to relevant data despite end-to-end encryption.

After a public hearing in 2017,[7] the justices rapporteurs issued their opinions in May 2020. In the Brazilian Supreme Court, the rapporteur is responsible for reviewing the case files and issuing an initial opinion that serves as a slate upon which the remaining justices will build until they reach a final decision. It is, therefore, a seriatim process where every justice writes her own individual opinion. There is no "opinion of the court." It is common for the rapporteurs to issue their opinions months (and sometimes years) before the court is ready to decide the case on the merits. In the WhatsApp cases, the rapporteurs highlighted the importance of data access to law enforcement agents, yet, at the same time, they underscored the significant role of encryption as a safeguard for certain rights, particularly the rights to privacy, inviolability of communications, and freedom of speech.

Justice Edson Fachin, one of the Rapporteurs, noted in his opinion[8] that encryption can buttress fundamental rights in democratic societies. He acknowledged that encryption is "the mechanism par excellence to guarantee the right to privacy" and noted that the only way to "disable encryption for one user is to disable it to all." Therefore, in his words, "to weaken encryption is to undermine the right of all to a safe internet."

Fachin argued that the imposition of solutions that involve exceptional access or that reduce the protection provided by strong encryption protocols are inconsistent with the Brazilian legal order. In his words,

> the risk caused by the use of cryptography does not yet justify the imposition of solutions that involve exceptional access or other solutions that reduce the protection guaranteed by strong cryptography. . . . There is no way to force internet applications that offer end-to-end encryption to break the confidentiality around the content of communication.

Justice Rosa Weber, the second rapporteur, advanced similar arguments in her decision.[9] For her, the fundamental freedom that grants individuals the right to close their house's doors and install curtains on their windows also entails a "fundamental right to encryption" in order to "safeguard one's right to privacy." In her view, it would amount to "an inadmissible contradiction . . . to make it illegal or to limit the use of cryptography." Additionally, she stresses that end-to-end encryption does not prompt a trade-off between public security and privacy. In the long run, weaker encryption protocols expose the network and its users to even greater risks, ultimately undermining security.

It is important to note that both proceedings were stayed at the request of Justice Alexandre de Moraes. At the Brazilian Supreme Court, the justices have the power to suspend a case in order to further review the case's files before coming to a conclusion on the merits. This is known as a *pedido de vista*, or request for examination. It is also noteworthy that, before joining the court, Moraes served as minister of justice in former president Michel Temer's cabinet. At that time, Moraes stated in an interview that internet companies should be prepared to hand over information whenever it was deemed necessary to fulfill purposes of law enforcement.[10] It is unclear whether he will hold this position now as a justice on the Supreme Court. While the cases are still pending, the direction given by the rapporteurs is that encryption advances other rights such as the right to privacy and data protection. Therefore, encryption should not be weakened at the expense of these other rights.

New Cases

Two other cases decided in 2020 by the Supreme Court support the argument in favor of encryption:

Brazilian Institute of Geography and Statistics

On May 7, 2020, the Brazilian Supreme Court issued an injunction suspending the Provisional Measure No. 954/2020 issued by President Jair Bolsonaro,[11] which mandated telecommunication companies to share a massive amount of personal data with the Brazilian Institute of Geography and Statistics (Instituto Brasileiro de Geografia e Estatística, IBGE). The justification for the provisional measure was the need to conduct a census through the phone since it is unsafe to conduct door-to-door inquiries during the pandemic. The court concluded that the measure was prima facie incompatible with the basic principles of privacy and data protection.

Even though the LGPD had not yet entered into force, a majority of the justices understood that the right to privacy and several principles of data protection were inherent to the constitution and serve as important safeguards that both the state and private enterprises should uphold. The majority decision argued that the measure did not cover: (i) clarity of the purpose of data processing; (ii) specificity on the necessity of the data requested; (iii) measures to mitigate risks; (iv) specific information regarding security measures; and (v) an accountability mechanism.[12]

This decision impacts the encryption debate in two ways. Firstly, it hardens the rights to privacy and data protection by enumerating both as protected under the constitution. This consequently makes it more burdensome for law enforcement agencies to advocate in favor of weaker encryption policies. Secondly, it reaffirms that principles of data protection also apply to the public administration. Hence, they shape and may even limit the ability of public officials to request access to encrypted data. If encryption supports the constitutional principles of privacy and data protection, then arguments to weaken encryption must be subject to a stricter scrutiny. It is necessary that public officials clearly demonstrate the existence of a public interest in accessing an encrypted data for law enforcement purposes.

Brazilian Intelligence Agency

In June 2020, the Brazilian Supreme Court heard a second case related to lawful access to encrypted data, this time involving the Brazilian Intelligence Agency (Agência Brasileira de Inteligência, ABIN). The case revolved around changes to ABIN's structure that expanded its powers to request data from

other organs of the government. This expansion was challenged before the court on grounds of violating the right to privacy, protection of personal data, and informational self-determination.

The majority of the justices decided that even in cases of data requests within the government for intelligence purposes, privacy and data protection should be at the forefront and may require particular procedures to be followed.[13] One justice rapporteur noted in her vote a parallel with wiretapping that, in her view, demands guarantees to protect individuals' privacy and personal data. The presiding justice underscored the need for safety protocols around data transfer. However, the justice stopped short of assessing whether encryption should be a component of such protocols, urging instead for an accountability mechanism in cases of abuse or omission.

Coupled with the IBGE case, this decision strengthens the argument in favor of encryption in Brazil. It stresses that, as a matter of constitutional law, the public interest in intelligence services does not automatically outweigh privacy and data protection concerns. Similarly, the ABIN case underscored that public officials should offer compelling evidence of the existence of a public interest in accessing encrypted data when the effectiveness of law enforcement may depend on it.

Outlook

Although the Supreme Court so far has pointed to a clear direction, it is too early to tell how the encryption debate will be settled in Brazil. After all, although the rapporteurs in both cases have issued pro-encryption opinions, it is unclear whether the remaining justices will follow their lead or join their peers in dissent. In a way, Moraes's request to suspend both cases can be perceived as a sign that the decision is unlikely to be unanimous. Furthermore, the executive and the legislative branches do not seem to be moving in the same direction, creating tensions between the three branches of government. The support for privacy and data protection even when intelligence services wish to access encrypted information seems to suggest, at least for the time being, that the Supreme Court is more likely to favor a higher degree of scrutiny toward any attempt to break or circumvent encryption.

About the Authors

Priscilla Silva is an attorney at law. She is a PhD candidate and holds a master's degree in constitutional law from Pontifical Catholic University of Rio de Janeiro. She was a writing fellow at the BYU Religion and the Rule of Law program at Oxford University. She is currently a researcher on the rights and technology team at the Institute for Technology and Society of Rio de Janeiro and a member of DROIT's law and technology research group.

Ana Lara Mangeth has a bachelor's degree in law from Pontifical Catholic University of Rio de Janeiro. She is a researcher in DROIT's law and technology group and has worked as a junior researcher on the rights and technology team at the Institute for Technology and Society of Rio de Janeiro.

Christian Perrone is a PhD candidate and Fulbright Scholar at Georgetown University., He holds a master's degree in law from Cambridge University and a Diploma of the Academy European University Institute on International Human Rights. He was previously a secretary for the Inter-American Juridical Committee and a human rights specialist at the Inter-American Commission on Human Rights, both part of the Organization of American States. Perrone is currently a coordinator with the rights and technology team at the Institute for Technology and Society of Rio de Janeiro.

About the Encryption Working Group

The Carnegie Endowment for International Peace and Princeton University have convened a small group of experts to advance a more constructive dialogue on encryption policy. The working group consists of former government officials, business representatives, privacy and civil rights advocates, law enforcement experts, and computer scientists. Observers from U.S. federal government agencies attended a select number of working group sessions. Since 2018, the working group has met to discuss a number of important issues related to encryption policy, including how the relevant technologies and uses of encryption will evolve in the future.

This brief and its companion pieces detailing the encryption debates in a select number of key countries and regions—Australia, Brazil, China, the European Union, Germany, and India—were prepared by local and area experts at the request of the Encryption Working Group. They are de-

signed to shine light on key drivers of the debates in these countries, how they have evolved in the last five years, and the divergent approaches taken by different governments. The briefs do not take a position on encryption policy, rather they provide analysis of how debates about encryption have evolved internationally. The views are the authors' own and do not necessarily reflect the views of Carnegie or the Encryption Working Group..

Notes

1 "Key Findings of the Internet & Jurisdiction and ECLAC: Regional Status Report 2020," UN Economic Commission for Latin America and the Caribbean, 2020, https://repositorio.cepal.org/bitstream/handle/11362/45732/4/S2000402_en.pdf; and "The Hamburg G20 Leaders' Statement on Countering Terrorism," G20 Information Centre, July 7, 2017, http://www.g20.utoronto.ca/2017/170707-counterterrorism.html.

2 Gabriel Aleixo, et al., "The Encryption Debate in Brazil," Carnegie Endowment for International Peace, May 30, 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219.

3 Priscilla Silva, "The Current Scenario of Data Protection Law in Brazil," ITS Rio, accessed March 16, 2021, https://itsrio.org/en/artigos/the-current-scenario-of-data-protection-law-in-brazil/.

4 "Marco Civil Law of the Internet in Brazil," Internet Steering Committee, April 24, 2014, https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180.

5 "Decree No. 8771, May 11, 2016," Internet Lab, https://www.internetlab.org.br/wp-content/uploads/2016/05/Decree-MarcoCivil-English.pdf.

6 "Ação Direta de Inconstitucionalidade 5527" [in Portuguese], Brazil's Supreme Federal Court, http://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282; and "Arguição de Descumprimento de Preceito Fundamental 403" [in Portuguese], Brazil's Supreme Federal Court, http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500.

7 "Definidos participantes e cronograma da audiência pública sobre WhatsApp e Marco Civil da Internet" [in Portuguese], Brazil's Supreme Federal Court, April 24, 2017, http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=341437.

8 "Arguição de Descumprimento De Preceito Fundamental 403 Sergipe" [in Portuguese], Brazil's Supreme Federal Court, http://www.stf.jus.br/arquivo/cms/bibliotecaConsultaProdutoBibliotecaPastaFachin/anexo/ADPF403voto.pdf.

9 "Ação Direta de Inconstitucionalidade 5.527 Distrito Federal" [in Portuguese], Brazil's Supreme Federal Court, http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf.

10 Nathalia Passarinho, "Governo elabora projeto para regular acesso a informações do WhatsApp" [in Portuguese], G1, July 17, 2016, http://g1.globo.com/politica/noticia/2016/07/governo-elabora-projeto-para-regular-acesso-informacoes-do-whatsapp.html.

11 "Medida Provisória n° 954, de 2020," National Congress of Brazil, https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619.

12 “STF suspende compartilhamento de dados de usuários de telefônicas com IBGE” [in Portuguese], Brazil’s Supreme Federal Court, May 7, 2020, http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902&%3A~%3Atext=O%20Plen%C3%A1rio%20do%20Supremo%20Tribunal%2Ca%20pandemia%20do%20novo%20coronav%C3%ADrus.

13 “STF impõe limites ao compartilhamento de dados do Sistema Brasileiro de Inteligência (Sisbin)” [in Portuguese], Brazil’s Supreme Federal Court, August 13, 2020, https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=449549&ori=1.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org