INTERNATIONAL ENCRYPTION BRIEF

MAY 2019

The Encryption Debate in Brazil

Gabriel Aleixo, Andrea Guimaraes Gobbato, Natalia Langennegger, Ronaldo Lemos, Isabela Garcia de Souza, and Fabro Steibel

The Encryption Debate in Brazil

Gabriel Aleixo, Andrea Guimaraes Gobbato,
Natalia Langennegger, Ronaldo Lemos,
Isabela Garcia de Souza, and Fabro Steibel

For your convenience, this document contains hyperlinked source notes as indicated by teal colored text.

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.

CONTENTS

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 briefing paper 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 designed 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.

The Encryption Working Group will continue its efforts to study this important issue and plans on releasing further briefings on aspects of the encryption policy debate.

Members of the Encryption Working Group include:

Jim Baker
Former General Counsel, Federal Bureau of Investigation

Katherine Charlet
Program Director, Technology and International Affairs, Carnegie Endowment for International Peace

Tom Donahue
Visiting Fellow, George Mason National Security Institute, and former Senior Director for Cyber Operations, National Security Council, White House

Ed Felten
Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University

Avril Haines
Senior Research Scholar at Columbia University's Columbia World Projects and former Deputy Director, Central Intelligence Agency

Susan Hennessey
Executive Editor, Lawfare, and Senior Fellow in Governance Studies, the Brookings Institution

Chris Inglis
Managing Director, Paladin Capital Group, and former Deputy Director, National Security Agency

Sean Joyce
US Cybersecurity and Privacy Leader, PwC, and former Deputy Director, Federal Bureau of Investigation

Susan Landau
Bridge Professor of Cyber Security and Policy, Tufts University

Christy Lopez
Distinguished Visitor from Practice, Georgetown Law Center

Alex Macgillivray
Board Member, Data & Society, and former Deputy Chief Technology Officer of the United States

Jason Matheny
Founding Director, Georgetown Center for Security and Emerging Technology, and former Director, Intelligence Advanced Research Projects Activity

Tim Maurer
Co-Director and Fellow, Cyber Policy Initiative, Carnegie Endowment for International Peace

Denis McDonough
Visiting Senior Fellow, Technology and International Affairs, Carnegie Endowment for International Peace, and former White House Chief of Staff

Lisa Monaco
Distinguished Senior Fellow, Reiss Center on Law and Security, New York University School of Law, and former Assistant to the President for Homeland Security and Counterterrorism

Laura Moy
Executive Director, Center on Privacy & Technology, Georgetown Law Center

Michelle Richardson
Director, Privacy and Data Project, Center for Democracy and Technology

Ronald L. Rivest
Institute Professor, Massachusetts Institute of Technology

Ari Schwartz
Managing Director of Cybersecurity Services, Venable LLP

Harlan Yu
Executive Director, Upturn

Denise Zheng
Senior Associate (Non-resident), Technology Policy Program, Center for Strategic and International Studies

Note: This is not a comprehensive list of all members. Some wish to remain anonymous for the time being and to contribute in their personal capacity.

Encryption has become an important issue in Brazil due to debates regarding the use of end-to-end encryption by app providers; the expansion of the cryptocurrencies market; and recent legislation on internet use, data protection, and privacy. This brief will explore these issues, present related policies, and examine the future of encryption in the country. So far, neither legislation nor judicial decisions have drawn a definitive line on access to encrypted data.

Introduction

The encryption debate in Brazil focuses on balancing the needs of law enforcement and the promotion of secure encryption systems. One of the main issues is the use of end-to-end encryption by communications applications (apps). Some companies have adopted technological architecture that inhibits the government's ability to obtain access to communications data that could be of use to officials investigating and prosecuting criminal activities. Brazilian judges have repeatedly ordered service providers to block the communications app WhatsApp in response to the company's (which is owned by Facebook) noncompliance with judicial decisions requiring it to provide information related to ongoing investigations. Two major cases have not yet been resolved.

Key Actors

One of the key institutions involved in the technical dimensions of cryptography is the Brazilian Computer Emergency Response Team (CERT), which is responsible for promoting the adoption of encryption to enhance cybersecurity. In addition, the National Communications Regulatory Agency (ANATEL) issued a resolution that requires telecommunications companies to incorporate encryption into their services. Another notable actor is the National Institute of Information Technology, which coordinates the development and management of cryptographic key certificates—specifically ICP-Brazil, a software for certifying digital signatures. Meanwhile, the Institutional Security Office (GSI), under the control of the president, is tasked with encrypting classified documents, guarding state-owned cryptographic systems, and delivering encrypted intelligence to end-to-end communications services. Lastly, the Central Bank of Brazil adopted a cybersecurity policy by way of a 2018 resolution, which reinforces requirements that cryptography be used for the sharing of financial data. None of the listed authorities has a specific mandate to order the breach of a third-party encrypted service. That issue depends on how the Supreme Federal Court rules on the two important ongoing cases pertaining to this issue (see below).

The encryption debate in Brazil is still incipient, and few experts outside of government are publicly engaged on this issue. Even in fields that typically address encryption, such as mathematics, the policy implications are not a prominent topic of conversation; the debate that is happening is being mainly driven by technical specialists, policy-focused experts, and organizations—including university professors, academic research groups, and representatives of civil society—that are discussing technology and the challenges it raises.

Some academics have tried to stimulate discussions on privacy issues. Diego Aranha, a specialist on encryption and computing security, is an advocate for privacy and data protection. His position is that there is no real conflict between privacy and public order, as is often alleged. Meanwhile, another professor named Sergei Popov draws attention to the need to update encryption systems. In this spirit, he has developed a cryptocurrency with a high-level encryption system, based on quantum computing, that uses the Winternitz hash-based signature scheme.

At the same time, privacy advocacy organizations support security in communications and question surveillance practices. Coding Rights, a women-run organization, helps facilitate debates about surveillance and privacy through various projects and conferences. They defend the use of encryption and oppose the employment of backdoors and key escrows, believing that allowing access through these tools would weaken security systems. Another organization, ITS Rio, researches encryption risks and organizes related online courses, conferences, and seminars. Mudamos, an app created by ITS Rio, aims to increase civic participation in the legislative process. It informs users about legislative schedules and enables them to petition draft bills that may be forwarded to the National Congress.

Legal Framework

Although encryption is obviously legal in Brazil (the temporary judicial bans of WhatsApp notwithstanding), there is no right to cryptography enshrined in the country's legal code. Legal provisions on privacy and secrecy in informatics date from the 1980s, and in the 1990s, end-to-end encryption was mostly framed as a security measure for individuals and organizations to establish trust (for banks or email service providers, for instance). The use of encryption as a security measure in the public sector is well regulated and is a key element of the digital identity ecosystem overseen by the government. The Brazilian Internet Steering Committee also promotes the use of cryptography as essential for protecting privacy, free expression, and human rights.

The first Brazilian legislation to reference data protection and secrecy was issued in 1984, but it was only after the enactment of a 2000 decree (establishing an information security policy for government agencies) that the state began issuing regulations on encryption. Subsequently, the government reworked a 2001 provisional measure, which created a public key infrastructure organization, ICP Brasil, specifically authorizing the use of digital signatures, a technology that requires cryptographic algorithms.

A second wave of relevant legislation, including the 2011 Access to Information Act (LAI), the 2014 Internet Bill of Rights (MCI), and the 2018 General Data Protection Law (LGPD), focused on data protection and privacy rights. The MCI legislation, in particular, was greatly influenced by the revelations that former U.S. national security contractor Edward Snowden made in 2013 concerning

U.S.-led worldwide electronic surveillance efforts, especially because then Brazilian president Dilma Rousseff was found to be one of the world leaders under NSA surveillance. More recently, the Cambridge Analytica–Facebook data-sharing scandal in the 2016 U.S. presidential election, Europe's passage of the General Data Protection Regulation (GDPR) in 2016, and Brazil's desire to join the OECD were crucial motivating factors for the enactment of the LGPD.

The LAI prescribes the classification of confidential information, and another 2012 decree regulates the procedures for processing confidential information and maintaining secrecy and requires the use of cryptography and state algorithms, or mathematical functions developed by the government to securely code and decode information of interest to public bodies. The MCI established network security as a principle for internet use in Brazil. A subsequent 2016 decree encourages internet providers to protect data by using encryption or equivalent measures. Finally, the LGPD also adopts network security as a principle, and its content relates to security practices, data pseudonymization, and privacy by design.

Data Localization

There is no provision for data localization in Brazilian federal law. The main debate around this issue took place in 2011 during the final round of congressional hearings preceding the passage of the MCI. The only legal provision of any kind for data localization is found in the norms for the Ministry of Planning and the GSI regarding government contracts related to information and communications, which may include encryption methods, firewalls, and other measures.[1] According to these rules, confidential data or information produced or safeguarded by the Federal Public Administration, including backup data, shall be physically located in Brazil.

The debate about data localization was recently reignited by two events. First, the Central Bank of Brazil issued a 2018 resolution that allows financial institutions to process and store data in the country or abroad, rather than insisting on data localization. Second, the National Council of Justice decided to suspend a contract established between the Court of Justice of São Paulo and Microsoft regarding cloud-computing services (a definitive decision on this dispute is still pending). The outcome of this decision may influence how Brazil is positioned in relation to data localization and foreign technology companies.

Main Issues

Internet Bill of Rights

A landmark passage of the MCI was the culmination of a drafting process that began years earlier. The product of the open and collaborative efforts of civil society groups who proactively proposed

it, this law represented an attempt to translate the principles of the Brazilian Constitution for the worldwide web.

The final version of the MCI protects rights such as net neutrality and privacy and aims to enact safeguards against mass surveillance. The law upholds freedom of expression, creating safe harbors for Brazilian online intermediaries, which are not held liable for content published by third parties unless a court orders them to take down specific content.[2] It also guarantees the inviolability and secrecy of users' online communications, permitting exceptions only by court order. At the same time, a 2016 decree, which codified the MCI into law, includes provisions for the use of technologies that guarantee the inviolability of data and encourages internet service providers (ISPs) and online service providers (OSPs) to adopt encryption for keeping, storing, and processing personal data and private communications.

WhatsApp Cases

The MCI has been challenged in the Brazilian court system, particularly in response to WhatsApp's use of end-to-end encryption. In 2015 and 2016, the courts blocked WhatsApp on and off on three different occasions, and the Brazilian Supreme Federal Court has gotten involved to decide whether these bans are legal. These orders were challenged on the grounds that they violated data protection regulations and infringed on freedom of speech, the right to privacy (including that of private online communications), and internet companies' business models. Because 76 percent of Brazilian smartphone owners use the app, the court orders were challenged on the grounds that the punishment was disproportional to the offense.

The cases reached the Supreme Federal Court, which called a public hearing on the topic.[3] The court asked experts to evaluate the pros and cons of implementing or building systemic backdoors into end-to-end cryptography systems, making use of exception access mechanisms, and providing unauthorized access to individuals' mobile communications. The court made no specific note on what type of vulnerability could be used, although comments from experts covered the upsides and downsides to using backdoors and lawful hacking.

During the hearing, encryption specialists, such as Diego Aranha, argued that the current framework on encryption was based on control, rather than security, and he further said that strong encryption is the cornerstone of the modern information economy's security and protects people against threats. In contrast, the government framed its interest in lawful hacking, backdoors, or other solutions in terms of efficiently conducting criminal investigations and prosecutions. Representatives from the Federal Police and from the Public Prosecutor's Office argued instead that encryption services should respond to court demands when required and that exceptional access measures should be available for data collection if necessary. Telecommunications company representatives sided with the security forces, adding that telecommunications services are required by law to provide such services, which are costly, and that internet services providers should face a similar

burden. One of the authors (Ronaldo Lemos) participated in the hearing and focused on the impact of app blocking on network infrastructure and on the importance of promoting privacy and freedom of expression at the content-level of the network.

Specialists outside of the government and representatives of civil society did not support this protocol modification. They argued that it would be inefficient, could potentially jeopardize the app's security, may cause problems with management due to its global scale, and could potentially infringe on users' personal rights.

In 2016, the Supreme Federal Court called on interested parties to participate in another public hearing, resulting in one of the main debates about encryption in Brazil. The court chose roughly twenty parties from among nearly 200 requests to attend the hearing. The selected hearing attendees included: (1) private sector companies (including WhatsApp, Facebook, and ISPs); (2) government entities, such as the Federal Police of Brazil, the Public Prosecution Service, the Ministry of Science, Technology, Innovation, and Communications, the Internet Steering Committee, and the Information and Coordination Study Group of Ponto BR (NIC.br); (3) academics (professors in the fields of computing, engineering and/or information security); (4) nonprofits (research institutions focused in legal issues, such as ITS RIO, InternetLab, and Lapin-UnB), and (5) civil society (judges and lawyers' associations).

Outlook

In spite of its importance, Brazil does not have a culture of employing encryption tools for personal use. In general, people rely on encryption provided by WhatsApp, iMessage, Telegram, and other apps.

Even though the encryption debate has only intensified in recent years, it is safe to say that this is only the beginning. The EU-promulgated GDPR has already boosted discussions about privacy. Brazil's equivalent legislation, the 2018 LGPD, will come into effect in 2020. The LGPD has been central to the debate on technology challenges, privacy, and data protection, and it also has called attention to encryption, blockchain, and other related technical issues.

Legislative action directly related to encryption are not typical, since few bills address the technology. Two pieces of legislation do address the modernization of health systems and state the requirement that electronic health records shall be protected by encryption.[4] Another similar act relates to payment methods and digital signatures in electronic commerce, using encryption to ensure that transactions are conducted securely.[5] Finally, another bill provides for the use of encryption in electronic judicial petitioning.[6]

It is difficult to say which stakeholders, issues, and technologies will be the most important drivers of the encryption debate, given that the debate is still incipient. Nevertheless, recent developments in cryptography can be viewed in terms of two factors: encryption used by the government to protect the privacy of its own communications and national security, and concerns about citizens' privacy and data protection.

In terms of how the government uses encryption, there was a paradigm shift in 2014. Following the NSA surveillance scandal, the Brazilian government increased its concerns about the secrecy of communications of high-level officials. It abandoned one of the cryptographic patterns for digital certificates from the Public Key System ICP-Brasil (V3), issued by the National Institute of Information Technology, and instead adopted new cryptographic systems, including CriptoGOV and cGOV. Both patterns were developed by the Brazilian Intelligence Agency (Abin) and use a portable cryptographic platform (PCPv2).

As for citizens' privacy, the outcome of the pending WhatsApp cases will be highly influential, since it may shape and drive encryption discussions in the future. On the one hand, encryption and secrecy of information may be reinforced if the court finds that end-to-end encryption is not to be interrupted. On the other hand, if the judges hold that online and encrypted communications may be intercepted, Brazil may face the risks of heightened internet control and the challenge of aligning the possible requirements of such control on a global scale.

Furthermore, the cryptocurrencies market may be an important driver of the encryption debate since it has been growing and expanding its services and technologies in Brazil. In 2017, Brazil became one of the world's most significant Bitcoin markets. The value of the digital currency skyrocketed in 2017 and attracted the attention of a wide array of investors before it fell substantially thereafter. At least one public company, the National Bank of Economic and Social Development, announced in 2018 that it would issue a token of its own for financial activities. In turn, the Department of Federal Revenue also issued a norm in 2018 authorizing the sharing of public administration data using blockchain.[7] This development is relevant to the encryption debate insofar as blockchain technology depends on encryption, which is gradually being incorporated for public and private uses.

There is still considerable uncertainty regarding the future of encryption in Brazil. Even though encryption tools and related technologies have been gradually adopted, the country's legal framework does not provide clear standards for its wide adoption. Notwithstanding the scarcity of specific legislation, the Supreme Federal Court's eventual rulings on the WhatsApp cases this year are expected to provide some judicial guidance on the matter.

About the Authors

Gabriel Aleixo has an undergraduate degree from FGV EBAPE, is a member of the Business Equilibrium Council in the area of innovation, serves as a business developer at A Star, and works as a senior researcher at ITS, leading projects involving Bitcoin, blockchain, and digital security.

Andréa Guimarães Gobbato is a law student at the University of São Paulo and works at Pereira Neto Macedo on issues related to the media, technology, and intellectual property.

Isabela Garcia de Souza is a law student at FGV São Paulo Law School and works at Pereira Neto Macedo on issues related to the media, technology, and intellectual property.

Natalia Langenegger is a PhD candidate at the University of São Paulo and has a master's degree in law and development from the FGV São Paulo Law School. She is a lawyer at Pereira Neto Macedo on issues related to the media, technology, and intellectual property.

Ronaldo Lemos holds a PhD in law from the University of São Paulo and a master's degree in law from Harvard University. He is a professor at Columbia University as well as director and one of the co-founders of the Institute for Technology and Society of Rio de Janeiro.

Fabro Steibel is a postdoctorate affiliate of the Berkman Klein Center at Harvard University, a member of the Global Council of the World Economic Forum, and the executive director of the Institute for Technology and Society of Rio de Janeiro.

The authors would like to thank Danilo Doneda and Jeferson Fued Nacif for reviewing the manuscript.

Notes

1 See GSI/PR Supplementary Norms no. 4 and 19; and MP/STI Ordinance no. 20/2016, MPOG.

2 That said, online platforms can be held liable for sexual content published by third parties without participants' authorization. Additionally, the alleged author may request that the platform remove copyright-infringing content, providing information about the authorship and indicating the offending webpage.

3 The two WhatsApp-related cases (ADI 5527 and ADPF 403) were received by the Supreme Federal Court in May 2016. After public hearings, the court's decisions are still pending.

4 See PL 471/2008 and PL 474/2008.

5 See PL 4906-A/2001.

6 See PL 3279/2012.

7 See Ordinance 1788/2018.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

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

CarnegieEndowment.org