INTERNETLAB
pesquisa em direito e tecnologia

São Paulo, February, 15, 2019.

To:

MANDATE OF THE UN SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION

Att.: Mr. David Kaye

Dear Mr. David Kaye,

In attention to the call for submissions on surveillance practices and human rights violations ("The Surveillance Industry and Human Rights") we hereby present a summary of InternetLab's main research findings concerning the local context in Brazil. InternetLab is an affiliated member of the Network of Centers, a global network of internet and society research centers, and has been conducting extensive research on state surveillance and digital rights in Brazil.

The present submission aims to provide an overview of the main weakenesses of the legal framework applicable to state surveillance in Brazil, with a particular focus on specific practices, loopholes and interpretations that undermine the protection of personal freedoms. In doing so, we hope to contribute to the work of the Rapporteur, indicating potential sources of reference and drawing your attention to the following issues:

1. **Brazilian law does not provide adequate standards of protection to stored private communications, metadata and account information of subscribers:**

    - The legal framework that establishes limitations on state surveillance of communications in Brazil is essentially derived from provisions of the Brazilian 1988 Federal Constitution; the Brazilian Civil Rights Framework for the Internet ("Marco Civil da Internet"); the General Telecommunications Law; the Law of Interceptions; the Criminal Procedure Code; besides specific provisions on other criminal laws. InternetLab's annual reports on State Surveillance of Communications provide a comprehensive analysis of the regulatory framework governing law enforcement access to communications data.[1]

[1] Abreu, Jacqueline de Souza, and Dennys Antonialli. 2017. "State Surveillance of Communications in Brazil." July 13. Available in: http://www.internetlab.org.br/en/biblioteca/report-state-surveillance-of-communications-in-brazil-2017/.

[2] "Article 5. All persons are equal before the law, without any distinction whatsoever, Brazilians and

edifício itália
avenida são luís 50
1º andar conjunto 11b
1046-000 são paulo sp brasil
www.internetlab.org.br

- Although the secrecy of communications is protected under the Brazilian Federal Constitution[2], there is significant dispute around the standards of protection conferred to different types of communications data. The main controversy lies on the scope of protection afforded under subsection XII of article 5 of the Brazilian Federal Constitution. The issue in question is whether the subject matter of protection of the secrecy of communications is the *actual content* - transmitted through correspondence, telegraph messages, data, and telephone calls; or the communication, understood as the *flow of such information while in transit*. The leading interpretations, supported by scholars[3] and endorsed by the Federal Supreme Court in RE 418.416-8/SC and HC 91.867/PA,[4] establishes that the protection under subsection XII applies only to the flow of communication while it is in transit, excluding of its scope the content and the corresponding metadata of communications.

- In keeping with this interpretation, the Law of Interceptions (Federal Law n. 9.296/96) establishes rigorous standards of protection for communications in transit, laying out specific and rigorous requirements for obtaining interception court orders.. The law establishes the circumstances, the requirements, the means and the time limit under which interceptions of communications are allowed.

- Under the Brazilian Civil Rights Framework for the Internet (article 7), access to stored private communications requires a court order. Differently from interception orders, however, there are no specific and substantive requirements of evidential standards that need to be fulfilled for these orders to be issued. Therefore, stored private communications may be subject to a lower degree of protection than *in transit communications* in Brazil.

---

[2] "Article 5. All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms:
[...]
X - the privacy, private life, honour and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured;
[...]
XII - the secrecy of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts."

[3] With respect to protection of flow of communications, it is worth noting FERRAZ JR., Tercio Sampaio's work, "Sigilo de Dados: o direito à privacidade and os limites da função fiscalizadora do Estado," in: Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, 1993, p. 439-459.

[4] In the trial of Recurso Extraordinário 418.416-8/SC, of 10/May/2006, the case reported by the Justice Sepúlveda Pertence states that protection under subsection XII of article 5 does not refer to information transmitted in correspondence, telegraph messages, data and telephone calls in itself but rather to communications in transit, to the flow of communications as they occur. Implicitly, the decision excludes application of the exception set forth in subsection XII to article 5 to data flow. In the trial of Habeas Corpus 91.867/PA, of 24/Apr/2012, reported by the Justice Gilmar Mendes, the interpretation of the secrecy of communications as protecting only the flow was reiterated.

- Other types of data, such as metadata and account information of subscribers, may receive even lower standards of protection. Loopholes in the legislation allow for warrantless law enforcement access of such data under different circumstances.[5]

- Different draft bills have been proposed in Congress to make these safeguards even weaker. On February, 4, 2019, Brazilian Minister of Justice Sergio Moro has released an anti-crime bill which seeks to amend the Law of Interceptions.[6] The amendments would include an article 9-A in the law in order to allow informatic and telematic interceptions, that could be conducted by any available technological mean, including the possibility of apprehension of stored communications data.

- Given that the development of mobile phones and smartphones have changed the circumstances under which law enfocerment investigations are conducted, the access to these different types of stored communications data enable new forms of surveillance. In addition to communication interceptions, access to metadata and stored communications have become a common practice.[7]

**2. Brazilian courts have been establishing precedents that broaden state surveillance capabilities and undermine safeguards to personal freedoms:**

- The interpretation that the constitucional secrecy of communications would also confer protection to the *content* of stored private communications has been refuted in different rulings by superior courts. In 2012, the Federal

[5] The Criminal Organizations Law (art. 15) and the Money Laundering Crimes Law (art. 17-B) authorizes police authorities and Public Attorney's Office's to request account information on the course of investigations of such crimes without a court order. Nevertheless, law enforcement authorities have been arguing that the Federal Law n. 12.830/2013, under article 2 §2, authorizes the Chief of Police to request informations and data that are relevant to any criminal investigation. Furthermore, since the enactment of the Criminal Organizations Law, authorities with appropriate jurisdiction, but especially chiefs of civil police, have also requested telephone logs from telephone companies without court orders, based on their combined interpretation of articles 15, 17, and 21 of this law. The constitutionality of these provisions both from the Criminal Organizations Law and the Federal Law n. 12.830/2013 are being challenged before the Federal Supreme Court through the Direct Actions of Unconstitutionality n. 5063/DF and n. 5059/DF.

[6] The project is available at: http://www.justica.gov.br/news/collective-nitf-content-1549284631.06/projeto-de-lei-anticrime.pdf.

[7] A complete analysis of the ways in which the "smartphone revolution" has enabled new forms of surveillance in Brazil is available in Abreu, Jacqueline de Souza / Antonialli, Dennys "The Treasure Trove's Tale: A Study on the Evolution and Popularization of Phones and Law Enforcement Access to Communications in Brazil." In: Sbramanian, Ramesh and Stefanie Felsberger (eds.). Mobile Technologies and Access to Knowledge, forthcoming.

Supreme Court (STF) established that the analysis of telephone records (metadata) of a cell phone seized in a flagrante arrest does not characterize a violation to the secrecy of communications.[8] In 2007, under the same case, at the trial of Habeas Corpus no. 66.368/PA, the Superior Court of Justice (STJ), had already decided in a similar manner.[9] Also, in a trial in September 2016, the STJ has refuted the enforcement of this constitutional secrecy upon the content of communication, affirming, in the same decision, the legality of evidence obtained in cell phones seized in the Car Wash Investigation upon a search and seizure warrant, even without the specific judicial authorization that limited the "virtual search".[10]

- According to research conducted by InternetLab on access to stored data on cellphones on "stops and frisks" and during searches incidents to arrest, in general, state courts have been endorsing the access to stored data without a court order, under the adoption of lesser protective legal interpretations against state surveillance, such as the limitation of the scope of protection of the constitucional secrecy of communications only to ongoing, and not to stored, communications. Also, state courts have been deemed these "virtual searches" legal under provisions of the Criminal Procedure Code that authorizes seizure on flagrante delicto arrest situations (art. 6), and under a supposed "presumption of consent" of the investigated. Neither the STJ more protective decisions, nor the guaranteed under the Brazilian Civil Rights Framework for the Internet seems to have had much impact on state courts decisions. [11]

- The level of protection applicable to data stored on electronic devices against state surveillance will be analysed, one more time, by the Federal Supreme Court on 13th march 2019, at the trial of RE 1.042.075, whose general repercussion has already been acknowledge. Under this case, the court will decide the lawfulness of the access to stored data on a mobile phone found at the crime scene. The state court decision on the case have already

[8] Federal Supreme Court. Habeas Corpus no. 91.867/SP. Rap. judge Gilmar Mendes, julg. 24.04.2012. Available at: <http://www.internetlab.org.br/wp-content/uploads/2019/02/HC-91.867.pdf>.
[9] Superior Court of Justice. Habeas Corpus no. 66.368/PA. Rap. judge Gilson Dipp, 5th panel, trialed on 05.06.2007. Available at: <http://www.internetlab.org.br/wp-content/uploads/2019/02/hc-66.368.pdf>.
[10] Superior Court of Justice. Appeal in Habeas Corpus no. 75.800/PR. Minister Felix Fischer, trialed on 15.09.2016. Available at: <http://www.internetlab.org.br/wp-content/uploads/2016/11/lavajato.pdf>. The decision was critically commented in Antonially, Dennys; Francisco Brito Cruz; and Mariana Giorgetti Valente. 2016. "Smartphones: treasure chests of the Lava-Jato investigation". In Deu nos Autos, November 24th 2016. Available in: <http://www.internetlab.org.br/en/opinion/smartphones-treasure-chests-of-the-lava-jato-investigation/>.
[11] Antonialli, Dennys; Jacqueline de Souza Abreu; Heloisa Massaro and Maria Luciano. 2018 "'Stop and frisks', searches incident to arrest, and law enforcement access to cellphones: overview and analysis of state courts case law." Revista Brasileira de Ciências Criminais, forthcoming.

deemed illegal the proofs obtained through the access to the data stored on the cellphone.

**3. The right to use strong end-to-end encryption technologies is under attack:**

- Brazilian law enforcement and judicial authorities have been exerting constant pressure on developers of products and services which promote and enable the adoption of strong end-to-end encryption technologies, particularly messaging services like WhatsApp and Telegram. Claiming that end-to-end encryption has been a major obstacle to criminal investigations, law enforcement authorities demand the development of technical solutions which would provide them with special access to the content of private communications. Over the last couple of years, Brazilian judicial authorities have sided with law enforcement demands, adopting drastic measures to compel WhatsApp, Brazil's most popular messaging service, to comply with users data requests. Courts have ordered that access to the messaging service be blocked several times. That happened, for instance, for forty-eight hours in December 2015[12], for seventy-two hours in May 2016[13], and indefinitely on July 19, 2016[14]. Each time, the suspension was prompted by WhatsApp's failure to comply with the Brazilian government's requests for data relevant to criminal investigations.[15]

- The imposure of such drastic measures has raised a national controversy and the Brazilian Federal Supreme Court has been called on to declare the blocks unconstitutional [16] Constitutional complaint ADPF 403[17] discusses the compatibility of judicial orders demanding blocks on WhatsApp with the right to freedom of communication, whereas ADI 5527[18] discusses the

[12] Reuters. Brazil court orders phone companies to block WhatsApp message app. December 16, 2015. Available at: <https://www.reuters.com/article/brazil-whatsapp-ban-idUSL1N1453JM20151217>.
[13] Reuters. Brazil judge orders WhatsApp blocked, affecting 100 million users. May 2, 2016. Available at: <https://www.reuters.com/article/us-facebook-brazil-whatsapp-idUSKCN0XT1KB>.
[14] Reuters. Brazil judge briefly blocks WhatsApp over criminal case. July 19, 2016. Available at: <https://www.reuters.com/article/us-brazil-facebook-whatsapp-ruling-idUSKCN0ZZ2PQ>.
[15] Abreu, Jacqueline de Souza. From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp. February 13, 2017. Available at: <http://btlj.org/2017/02/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/>.
[16] Folha de S. Paulo. Advogado vão ao STF para tentar blindar o WhatsApp de bloqueio. July 19, 2016. Available at: <https://www1.folha.uol.com.br/mercado/2016/07/1793239-advogados-vao-ao-stf-para-tentar-blindar-o-whatsapp-de-bloqueios.shtml>.
[17] Bloqueios.info. ADPF 403 IN STF: are WhatsApp blockings constitutional. November 21, 2016. Available: <http://bloqueios.info/en/adpf-403-in-stf-are-whatsapp-blockings-constitutional/>.
[18] Bloqueios.info. ADI 5527 and appblocks: a problem in the wording of the law or in its interpretation? November 18, 2018. Available at: <http://bloqueios.info/en/adi-5527-and-appblocks-a-problem-in-the-wording-of-the-law-or-in-its-interpretation/>.

constitutionality of items III and IV of art. 12 of the Brazilian Internet Civil Rights Framework (*Marco Civil da Internet*)[19], which authorizes the imposition of sanctions of "temporary suspension" and "prohibition of exercising activities" to internet connection and application providers that violate data protection rules. Both complaints are still pending.

- Yet there is no explicit ban on the use of end-to-end encryption technologies in Brazil, government officials have voiced strong intentions to regulate and restrict its use.

**4. Increasing adoption of privately developed facial recognition technologies in public services and in public safety policies and programs:**

- Public Administration has been increasingly adopting facial recognition technologies in public services. Accross the country, cities have started to implement facial recognition software to prevent fraud on buses.[20] These biometric transport systems are largely the product of public-private partnerships. Airports have also implemented similar technologies for international flights[21]. Schools have been using facial recognition to keep track of students attendance. The city of Jaboatão, in the state of Pernambuco, implemented the technology on all its public schools in 2017.[22] This year, a draft bill[23] proposing to implement similar technologies all over the country was introduced in Congress.

- Facial recognition technologies have also been the focus of public safety policies. In 2014, the state of São Paulo launched the "DETECTA program", based on the acquisition of a privately developed security system with intelligent cameras capable of identifying "suspicious activities" of civilians and reporting them directly to the law enforcement authorities.[24] In 2019 the city of Rio de Janeiro announced that will monitor the crowds during Carnival

[19] English translation available at: <https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf>.
[20] UOL. Ônibus adotam biometria facial em todo o Brasil para evitar fraudes. December 18, 2015. Available at: <https://gizmodo.uol.com.br/onibus-e-biometria-facial/>.
[21] G1. Aeroporto de Brasília passa a adotar reconhecimento facial de viajantes. August 1st, 2016. Available at: <http://g1.globo.com/distrito-federal/noticia/2016/08/aeroporto-de-brasilia-passa-adotar-reconhecimento-facial-de-viajantes.html>.
[22] G1. Escolas municipais de Jaboatão adotam reconhecimento facial para controlar frequência de alunos. April 18, 2017. Available at: <https://g1.globo.com/pernambuco/noticia/escolas-municipais-de-jaboatao-adotam-reconhecimento-facial-para-controlar-frequencia-de-alunos.ghtml>.
[23] Available at: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2191661>
[24] Folha de S. Paulo. Alckmin vai relançar sistema que já custou R$ 30 milhões e não funciona. June 30, 2017. Available at: <https://www1.folha.uol.com.br/cotidiano/2017/06/1897306-alckmin-vai-relancar-sistema-que-ja-custou-r-30-milhoes-e-nao-funciona.shtml>.

via facial recognition software.[25].It has also been reported that a few Brazilian Congressmen received an invitation to travel to China to be introduced to the latest developments on facial recognition systems.[26]

5. **Increasing adoption of surveillance drones (unmanned aerial systems) by law enforcement and intelligence agencies, without clear safeguards for the right to privacy:**

- International sports events seem to have set the stage for the use of surveillance drones in Brazil. For the occasion of the 2014 World Cup, a national integrated command center was created to monitor the cities and integrate several public databases, bringing together several law enforcement agencies and intelligence bodies, such as the military, civil and traffic police, fire and emergency departments and the Brazilian Intelligence Agency.[27] During the 2016 Olympic Games, surveillance drones were used to monitor and police Rio's airspace[28] and ANATEL authorized[29] the military to jam radio signals for security purposes. At the same time, surveillance balloons equipped with 13 high resolution cameras monitored a radius of 4 km, being able to accurately identify details such as car plates, guns and knives.[30]

- There has been a steady increase in the acquisition and use of surveillance drones as part of public safety operations. It has been reported that the Federal Police uses drones for complex criminal investigations, such as the operation involving a chief drug dealer at Complexo da Maré.[31] The city of São Paulo has also been an enthusiastic adopter of the technology, having

[25] Fast Company. Brazil is using facial recognition system during Rio's carnival. January 30, 2019. Available at: <https://www1.folha.uol.com.br/cotidiano/2017/06/1897306-alckmin-vai-relancar-sistema-que-ja-custou-r-30-milhoes-e-nao-funciona.shtml>.
[26] Folha de S. Paulo. Analistas veem risco à privacidade com tecnologia de reconhecimento facial. January 17, 2019. Available at: <https://www1.folha.uol.com.br/cotidiano/2017/06/1897306-alckmin-vai-relancar-sistema-que-ja-custou-r-30-milhoes-e-nao-funciona.shtml>.
[27] World Cup Portal. National Integrated Command and Control Center will coordinate security actions during the World Cup. May 25, 2014. Available at: <http://www.copa2014.gov.br/en/noticia/national-integrated-command-and-control-centre-will-coordinate-security-actions-during-world>.
[28] O Globo. Drones reforçam segurança do espaço aéreo do Rio. August 4, 2016. Available at: <https://oglobo.globo.com/rio/drones-reforcam-seguranca-do-espaco-aereo-no-rio-19848806>.
[29] The Verge. How Brazil is trying (and failing) to keep drones away from the Olympics. August 8, 2016. Available at: <https://www.theverge.com/2016/8/8/12402972/olympics-rio-2016-anti-drone-jamming-public-safety>.
[30] UOL. Falta de limites sobre balões vigilantes nas Olimpíadas põe privacidade da população em xeque. August 5, 2016. Available at: <https://gizmodo.uol.com.br/baloes-vigilantes-olimpiadas-rio-2016/>.
[31] UOL. PF utilizou drone para investigar chefe do tráfico do Complexo da Maré. March 27, 2014. Available at: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2014/03/27/pf-utilizou-drone-para-investigar-chefe-do-trafico-do-complexo-da-mare.htm>.

used surveillance drones to monitor protests and crowded public events[32] such as street Carnival.[33]

- Even tough the National Agency for Civil Aviation (ANAC) established rules for the use of drones in Brazil, their use for military and public safety purposes falls outside the scope of the regulation. [34]

***

We hope this submission provides relevant insights to the work of the Rapporteur. Please do not hesitate to contact us should we can be of any further assistance.

**Dennys Antonialli**
*Executive Director*

**Thiago Dias Oliva**
*Head of Research*

**Maria Luciano**
*Researcher*

**Heloisa Massaro**
*Researcher*

[32] G1. Prefeitura de SP usa drones para vigiar de Cracolândia e Marcha para Jesus a manifestações. August 11, 2017. Available at: <https://g1.globo.com/tecnologia/noticia/prefeitura-de-sp-usa-drones-para-vigiar-de-cracolandia-e-marcha-para-jesus-a-manifestacoes.ghtml>.
[33] O Estado de S. Paulo. Doria estima renda de R$ 600 mi com carnaval e coloca drones para contar público nos blocos. February 10, 2019. Available at: <https://sao-paulo.estadao.com.br/noticias/geral,doria-estima-renda-de-r-600-mi-com-carnaval-e-coloca-drones-para-contar-publico-nos-blocos,70002185212>.
[34] Brazilian Regulation of Special Civil Aviation ("Regulamento Brasileiro de Aviação Civil Especial" (RBAC) nº 94") available at: <http://www.anac.gov.br/assuntos/legislacao/legislacao-1/rbha-e-rbac/rbac/rbac-e-94-emd-00>.