June 2015

Privacy International's comments on the Brazil draft law on processing of personal data to protect the personality and dignity of natural persons

1. Introduction

This submission is made by Privacy International.

Privacy International is a UK registered charity based in London. Privacy International is committed to fighting for the right to privacy across the world. We investigate the secret world of government surveillance and expose the companies enabling it. We litigate to ensure that surveillance is consistent with the rule of law and international standards. We advocate for strong national, regional, and international laws that protect privacy. We conduct research to catalyse policy change. We raise awareness about technologies and laws that place privacy at risk, to ensure that the public is informed and engaged.

Protecting privacy in the modern era is essential to effective and good democratic governance. This is why data protection law exists in over 100 countries worldwide. Further, protection of personal data is regulated in a range of international and regional instruments.[1]

Privacy International welcomes the efforts by Brazil to provide protections for the right to privacy, already enshrined in the Constitution of Brazil. PI welcomes the main aim of this law, namely to regulate the processing of personal data in order to protect the "fundamental rights of freedom and privacy of natural persons." (Article 1.)

Based on our experiences of working on privacy for over 25 years, our expertise on international principles and standards applicable to the protection of personal data, our leadership and research on modern technologies and data processing, Privacy International wishes to make a number of observations and recommendations on the draft law.

If you would like to discuss this submission of comments further, please do not hesitate to contact: Tomaso Falchetta, Legal Officer, tomasof@privacyinternational.org

1 See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

Comments on the draft Bill[2]

2. Independent Authority

In some Articles the bill makes references to a 'competent body,' without otherwise establishing or identifying it.[3] Article 21 of the Bill references other laws that may provide protection, but such protection is not defined and include vague terms such as "other instruments for individuals and collective protection".

The Bill should provide for the establishment of an independent data protection authority to supervise the way in which a body uses personal data. Such an authority is essential in order to ensure the enforcement of the data protection framework. Without this body, we have reason to doubt the sincerity and the effectiveness of this Bill altogether and the public would have no confidence in achieving any gains in privacy protection.

This authority must be given the mandate to conduct investigations and act on complaints by issuing binding orders and imposing penalties when it discovers an institution or other body has broken the law. Both individuals and public interest/privacy associations should be given the right to lodge complaints with this independent authority. The independent authority should also be able to receive complaints of competent organisations based on evidence revealing bad practice before a breach has occurred.

The Bill should identify the composition of this authority, including the skills and expertise required. Further, the Bill must stipulate that the independent data protection authority will be given sufficient resources, both financial and human, and remain administratively independent, to effectively and adequately fulfill its mission of enforcing the data protection framework.

The independent authority must have the power to must have the power to impose appropriate penalties, and provide compensation for material and non-material damages suffered. Article 50 lists a number of administrative penalties. However, it is not clear whether these penalties will only be imposed following a complaint by the data subject, and there is no specification of the overall fines (including a maximum penalty or, ideally, a percentage of the company's turnover.)

3. Scope of the Bill

Article 2 – Exception for journalistic purposes

> "§ 2 This Law does not apply to any data processing that is: […] II - Performed for exclusively journalistic purposes."

The "journalist exemption" in Article 2 paragraph 2 is too narrow. Privacy International suggests that it includes other legitimate exercises of freedom of expression, such as

2 http://participacao.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/02/Brazil_pdp_bill_Eng1.pdf
3 See Articles 10, 13, 15,15,18 and 50.

investigations carried out by independent non-governmental organisations. As such, Privacy International recommends that this exception is broadened to include "performed for journalistic, artistic/literary expression, or other freedom of expression or human rights purposes".

Article 4 – Exemption for state security and criminal investigation

> "Processing of personal data solely for purposes of public safety, defence, State security, research activities, or the repression of criminal offences, shall be governed by specific legislation, according to the general principles of the protection of the data subject's rights established in this Law."

Privacy International recommends that the bill develops and lists the standards applicable to the protection of personal data collected and processed for the purposes of public safety, defence, state security and investigation or prevention of criminal offences. Such standards should at a minimum identify the public bodies mandated to collect and process personal data, fully respect and protect the right to privacy, and comply with the principles of legality, necessity and proportionality identified by international human rights experts.

Alternatively, this provision should clarify that in the absence of specific legislation, any collection and processing of personal data for the purposes of public safety, defence, state security and investigation or prevention of criminal offences shall only be conducted in compliance with the provisions in this bill.

3. Definitions

Article 5 - Definitions

Paragraph I - Personal data

> "I - personal data: any data related to an identified or identifiable natural person, including identification numbers, location data, or electronic identifiers;"

Privacy International recommends this definition be expanded and strengthened to clarify that any information used to identify an individual renders that information personal data. For example, profiling, tracking and monitoring do not need a specific name/address or other direct identifier, but they can still be used to identify individuals and affect how they are treated. Privacy International suggests the following alternative language: "personal data shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity."

Paragraph III – sensitive data

> "III - sensitive data: personal data that disclose the person's racial or ethnic

> origin, religious, philosophical, or moral beliefs, political views, affiliation to trade unions or religious, philosophical, or political organisations, data pertaining to the person's health or sexual life, as well as genetic data;"

Privacy International welcomes the inclusion of the categories of sensitive data already identified in the draft law. We would suggest to add also a reference to data pertaining to the commission or alleged commission by the person of any offence.

Profiling

There is no definition of "profiling" in the draft Bill. With the rich history of challenges in profiling, and the prospect and challenges of innovation in data mining and machine learning, it is essential that protections are placed within this Bill. Privacy International recommends that a definition is included, using the language proposed by the European Parliament on the draft revised EU Data Protection Regulation. As such, the text would read as follow:

"profiling means any form of automated processing intended to evaluate, or generate data about, aspects relating to natural persons or to analyse or predict a natural person's performance at work, economic situation, location, health, preferences, reliability, behaviour or personality."

4. General Principles

Article 6 – General Principles

Principle of purpose

> "I - Principle of purpose, by which the processing must be performed for legitimate, specific, and explicit purposes that are known to the data subject;"

Privacy International recommends the addition to this principle that personal data must not be further processed or used in a way incompatible with such purposes.

Principle of necessity

> "III - Principle of necessity, by which the processing must be restricted to the minimum required for the performance of the purposes sought, including relevant, proportional, and non-excessive data;"

Privacy International suggests that this principle includes specifically that personal data should only be retained for no longer than is required for the purpose for which those data are collected and stored (see Council of Europe Convention No. 108.) This will strengthen and clarify the obligation to delete data at the end of processing (Article 15.)

Principle of free access

> "IV - Principle of free access, by which facilitated queries by the data subjects on the types of processing and on the integrity of their personal data must be ensured, free of charge;"

Privacy International suggests that this principle be amended to include an explicit right of the data subject to access personal data held on them. This will complement Article 17 (II) on the right of data subject to access to their personal data.

Principle of data quality:

> "V - Principle of data quality, by which the accuracy, clarity, and up-to-date nature of the data must be ensured, with the frequency required for the fulfillment of the purpose of the processing of the data;"

Privacy International recommends the inclusion of a requirement that every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. This will complement Article 17 (III) on the right of data subjects to correct incomplete, inaccurate or outdated data.

Principle of transparency:

> "§ 1 The public bodies shall announce their data processing activities by means of clear, precise, and updated information in easy accessible vehicles, preferably on its electronic websites, in compliance with the principle of transparency established in section VI."

Privacy International suggests that this important provision of transparency applies to all processors of personal data, whether public or private entities.

Principle of lawfulness and fairness:

The draft bill does not include the principle of lawfulness and fairness in obtaining and processing personal data, an important principle that is key to address practices such as the selling and/or transfer of personal data fraudulently obtained. As such, Privacy International recommends that the draft bill adds a principle of lawfulness and fairness, in line with international data protection standards such as the OECD Guidelines, and the Council of Europe Convention No. 108, along the following lines:

"Principle of lawfulness and fairness, by which personal data must be obtained and shared by lawful and fair means."

5. Requirements for personal data processing

Article 7 – consent

Privacy International welcomes the inclusion of strong provisions to ensure consent of the data subject. It would be useful to clarify that if the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

> "§6 Consent may be revoked at any time, free of cost to the data subject."

With regards to revocation of consent (paragraph 6), Privacy International recommends

that the provision clarifies that revocation of consent should lead to the deletion of the personal data (unless such consent was not required by the law). This will complement the provision in Article 17 (paragraph 4.)

Article 9 – Consent for children (under 12 years old)

> "Art. 9 In the case of data subjects of personal data who are not yet twelve years old, consent shall be given by their parents or legal tutors. The processing shall respect their condition as developing persons."

Privacy International suggests that this provision is strengthened by requiring the data controller to obtain verifiable forms of consent, as research suggests children may lie about their age or pretend to be their parents to access certain services.

The Bill should require that the "competent authority" develops standards and guidelines on this.

Article 10 – Information to the data subject

Privacy International welcomes this provision that illustrates the information that data subject should be provided and as such supports the data subjects' rights identified in Articles 17 and 18. The key issue is to identify how this will be done in practice. The draft Bill could, in this regard, require the "competent authority" to provide guidelines on this issue.

Article 13 – Sensitive Personal Data

> "Art. 13. The competent body may establish additional measures for the security and protection of sensitive personal data, which shall be adopted by the controller or by other processing agents.
>
> § 1 The performance of certain types of processing of sensitive personal data may be subject to the previous consent by the competent body, under the terms of the regulations.
>
> § 2 The processing of biometric personal data shall be regulated by the competent body, which shall establish the cases in which biometric data shall be regarded as sensitive personal data."

Privacy International recommends that the safeguards in this Article be strengthened. In particular, it would be advisable to specify that any processing that may disclose personal data without the consent of the data subject must only be carried out for the legitimate reasons described in the law and cannot result in the sensitive personal data being processed for other purposes or by parties other than those identified in the law. For example, processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies.

Privacy International suggests that biometric personal data should always be regarded

as sensitive personal data. Leaving it to the discretion of unspecified competent body risks lowering the applicable standards and level of protection afforded to such data in the draft law.

In the era of data linkability, and de-anonymisation of data sets, we are greatly concerned that even information that is not initially sensitive could quickly become sensitive. Biometrics certainly require additional protections because of their unique ability to track individuals across systems, their inability to revoke, and the often sensitivity of the information held within and derived from biometrics. We are also concerned that other forms of data can be uniquely identifiable, such as the signature of our movements, our device identifiers, and these can be linkable between non-sensitive and sensitive transactions. This signature then becomes a problematic unique identifier, just as a biometric, linking a device to an individual to a health record. We recommend further guidance and thought in this domain and suggest that the Bill requires the independent "competent authority" to develop guidance and keep this issue under review.

6. Data subject rights

Articles 16 – 21 - Data subject rights

Privacy International welcomes these provisions and recommends that they are put further up in the text of this Bill as they should be seen as applying throughout and as underpinning all provisions in this Bill.

Article 19 on automated processing of personal data

Privacy International recommends that this provision be strengthened by providing data subjects with the right to object to profiling (whose definition is suggested above.) Automated profiling is one of the fastest developing technologies, used for targeted marketing, and understanding and predicting human behaviour, and is liable to result in discrimination, especially of the disadvantaged or the poor.

7. International Data Transfer

Article 28 – International Data Transfer

> "Art. 28. International transfer of personal data is only allowed for countries that provide a level of protection for personal data that is equivalent to the level established in this Law, with no prejudice to the following exceptions:
>
> I - When the transfer is necessary for international legal cooperation between public intelligence and investigation bodies, in accordance with instruments of international law;
>
> II - When the transfer is necessary for the protection of the data subject's or a third party's life or physical safety;
>
> III - When the competent body authorises the transfer under the terms of the

regulations;

IV - When the transfer is the result of a commitment assumed in an international cooperation agreement;

V - When the transfer is necessary for the execution of a public policy or fall within a public service's legal powers, in which case it should be publicly announced under the terms of section §1 of art. 6.

Sole paragraph. A country's level of data protection shall be assessed by the competent body, which shall take into account:

I - The general and sectorial standards established in the country's legislation;

II - The nature of the data;

III - Compliance with the general principles for personal data protection established in this Law;

IV - The adoption of security measures established in the regulations; and

V - Other specific factors pertaining to the transfer."

Privacy International recommends that the provisions in this Article be strengthened to ensure effective protection against the transfer of personal data to countries where such data may be used, processed or otherwise transferred in ways that infringe on the rights of the data subject.

Privacy International is concerned by the potentially broad exception of Article 28 IV. This exception needs to be construed narrowly to ensure that such agreements do not result in weakening the data protection offered in this Bill. Privacy International recommends that this exception is deleted and instead a provision is included in Article 29 specifying that international cooperation agreements that require transfer of personal data are without prejudice to this Bill.

Article 28 paragraph 1 should also not be construed as providing a broad exception to any forms of intelligence sharing.

Further, the assessment of the level of protection of personal data afforded in the third country (Article 28, sole paragraph) should include explicitly:

- rule of law, including national legislation in force and regulatory/professional rules;
- existence and effective functioning of independent supervisory authorities to ensure compliance with the law.