COMMENTS OF THE AMERICAN BAR ASSOCIATION SECTIONS OF ANTITRUST LAW AND INTERNATIONAL LAW ON THE PRELIMINARY BILLS FOR THE PROTECTION OF PERSONAL DATA FOR THE REPUBLIC OF BRAZIL

The views stated in these Comments are presented on behalf of the Section of Antitrust Law and Section on International Law. They have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and therefore should not be construed as representing the policy of the American Bar Association.

December 2, 2016

I. Introduction

The Sections of Antitrust Law and International Law (the “Sections”) of the American Bar Association respectfully submit these comments to the Bill of Law No. 330 (“Bill 330”) and the Bill of Law No. 5276/2016 (“Bill 5276”) (collectively the “Bills”), which are intended to provide a comprehensive data protection and data security framework for the Republic of Brazil.

In releasing this draft and soliciting public comment broadly, Brazil has encouraged a robust and informed dialogue to help contribute to the final configuration of the Bills. These comments are intended to further this dialogue and reflect the Sections’ experience in international and cross-border data protection and data security issues. The Sections’ long involvement in these issues rests on the participation of both private and public sector lawyers, economists, and market participants, reflecting the interests of all those who engage in, benefit from, and enforce legal rights relating to digital as well as traditional commerce in which personal data plays an important role. The Sections do not advocate on behalf of any particular interest, country, or party; rather, we offer our comments as constructive input of the type invited by the government of Brazil.

The Sections commend the government for the open process that characterizes law reform in Brazil in general, and the process surrounding the Bills in particular. We appreciate the changes made to the Bills based on comments submitted in April 2015 by the Sections, as well as many other commenters. The Sections also commend the government for the general consistency with international data protection law evidenced by the Bills. In these Comments, the Sections make several suggestions that we believe both further the goals of modernization and harmonization and serve the desired balance between individual privacy and the development of information markets and services that benefit Brazilian nationals and the development of a global marketplace.

II. Executive Summary

The Sections’ comments make the following suggestions:

- **Definition of “Personal Information” and “Sensitive Personal Information.”** We suggest that the Bills clarify the definition of information that will be considered personally identifiable and sensitive to be consistent with international norms.

- **Behavioral Profiling and Use of Non-Public Information.** We suggest modest changes to the Bills’ provisions concerning profiling to clarify that aggregate or anonymized data processing should not be regulated because it does not pose a risk of harm to identifiable individuals. We also suggest that the processing of non-
public information include exceptions for good faith (in addition to general derogations concerning free expression and legitimate research).

- **Written Consent.** We suggest that the processing of data based on legitimate grounds be emphasized as being on equal footing with other grounds, such as express written consent, and that implied consent be recognized as adequate in appropriate contexts.

- **Data Security.** We appreciate improvements made in these Bills but continue to recommend additional flexibility for their data security provisions, drawing upon the many years of experience in the United States with data security and breach notification laws.

- **The Rights of Data Subjects.** We make modest suggestions for improving the Bills’ treatment of the right to be forgotten and the right to data portability.

- **Big Data.** We suggest that several provisions in the Bills be reconsidered to facilitate “big data” analytics, which can provide important societal benefits.

- **Enforcement and Implementation.** We suggest minor changes in the enforcement and liability plan envisioned by the Bills.

We appreciate the opportunity to provide commentary to the government, and would be pleased to continue our participation or respond to any comments or inquiries that may be useful during this process.

III. Specific Suggestions

1. **Definitions of Personal Data and Sensitive Data**

   **Personal data.** Privacy laws in different jurisdictions adopt differing definitions of personal data, which may in turn affect the reach of their privacy laws. By delineating what information is (and, by exception, what is not) within the requirements and prohibitions of a privacy law, data gathering and processing practices may fall within or outside of the law’s reach.

   Privacy laws in different jurisdictions take somewhat different approaches to defining “personal information.” In the EU, personal data means any data relating to an identified or identifiable natural person. In the U.S., “personal data” is data that can be reasonably linked to a specific individual. In Singapore, personal data refers to data, whether true or not, about an individual who can be identified from that data. The definitions provided in both the Data Protection Directive and the General Data Protection Regulation (“GDPR”) imply that any data capable of being associated with an identifiable person will fall into the regime of personal data regulated under the privacy law.

   In the big data era, many countries have adopted the GDPR approach because an individual can be identified more easily now that data may be combined with other information or technology that reveals identity. The definition of personal data in the Bills is consistent with the GDPR,¹ which also provides a detailed definition of “an identifiable natural person”

---

¹ Bill of Law No. 5276/2016: “Personal data: data related to an identified or identifiable individual, including identification numbers, location data, or electronic identifiers that relate to an individual.”
following the definition of personal data. In Brazil’s Bills, there is no description on what constitutes an identified or identifiable individual. Thus, we recommend that the definition of identified or identifiable individual should be included in the Bills.

Sensitive data. Sensitive data encompasses a wide range of information, usually following EU law to include racial or ethnic origin, religious belief, sexual orientation, political opinions, trade union membership, and health. In a minority of countries outside of the EU, information about criminal offenses or, more rarely, civil offenses is added to the list. Other countries, such as the United States, add information about children and specific geolocation data to this list. Sensitive data involves basic rights of citizens and thus is generally protected with more restrictive rules than personal data. For example, the processing of sensitive data may be permissible only if the processor obtains explicit consent from the data subject prior to the processing of such data.

The definition of sensitive data in Article 5 (III) of Bill 5276 is generally consistent with EU-based norms. However, the Sections note that the word “REVEAL” (which affects the scope of sensitive data) was replaced by “CONCERNING”, which potentially expands the scope of the stricter protective rules applied to sensitive data.

2. Behavioral Profiling

Behavioral profiling is generally used to predict or measure individual behavioral preferences. It can be used in many scenarios, such as in recruitment for employment, marketing offers, and advertising. This type of profiling predicts the personality and future behavior of an individual based on specific data. The data used to build a behavioral profile, as provided in Article 13 (§1) of Bill 5276, may also be deemed personal data even if the data subject cannot be identified.

Use of such data are likely to affect the individual negatively if the data already incorporate bias or discrimination. However, the Sections respectfully suggest that Article 13 (§1) of Bill 5276 is not necessary because the risk of harm to an individual associated with behavioral profiling cannot arise if the data cannot be associated with an identifiable individual. Such data, therefore, need not be protected by privacy law. Accordingly, we recommend deleting Article 13 (§1) of Bill 5276.

3. Treatment of Publicly Available Information

Where information has been published or broadcast to the public, is available on request to the public, is accessible online or through other methods, or is available to the public by subscription or purchase, etc., such information is treated as publicly available. However, these data should be treated as publicly available information for purposes of privacy laws only if the data or information became publicly accessible lawfully and by legitimate means. The fact that a wide range of people can access the information does not necessarily mean that it was made available lawfully or by legitimate means. For example, a large amount of personal data that a company or an organization possesses may be disclosed to the public in a hacker attack. The processing or reuse of such data should not be subject to the publicly available data exemption.

---

2 An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
from privacy law restrictions (unless other exemptions apply, such as those relating to free speech or research). In practice, therefore, it is necessary to determine whether there is a legitimate source of publicly available personal data.

It may be infeasible to place the burden on users or recipients to verify whether data was made publicly accessible through a legitimate source because they may not have the same visibility into the original data source as the original processors. One practical way to deal with this issue is to hold that users can process the publicly available data provided that they access and use the data in good faith. This means the publicly available data can be freely processed unless in an intentionally negative way or unless the users know or should have known that the data was not lawfully released to the public. The Sections therefore respectfully suggest that Article 7 (§4) of Bill 5276, should be revised to provide that publicly available personal data may be used only when it is accessed and used in good faith. We suggest that the purpose for which the data were provided, or public interest reasons, should not affect whether the data can be used and should be removed from the provision.

4. **Data Anonymization**

Anonymous data appropriately falls outside of privacy law. Bill 5276 defines anonymized data as “data relating to a data subject that must not be identified.” Nevertheless, Bill 5276 uses different wording when it comes to the definition of anonymization. Anonymization implies any procedure whereby data may no longer be directly or indirectly associated with “an individual.” However, the Sections respectfully suggest that anonymization should require removal of any association with “an identified or identifiable individual”, not simply “an individual”. Information which directly or indirectly relates to an individual may not necessarily be associated with an identified individual. This clarification also would make the provision consistent with the definition of personal data.

Both Bills provide that anonymous data still shall be treated as personal data if the identity of the individual can be revealed through reasonable efforts. Today, data may be identified through certain technologies, mechanisms or procedures even if they have been initially anonymized. This poses a significant challenge to the protection of personal data. It is reasonable to include such data in the coverage of legislative protection.

However, the predicament, in practice, is how to define the standard of “reasonable efforts” used to reveal an identifiable individual. If reasonable effort includes the use of techniques or technologies that require a significant investment of capital, the scope of regulated data under Bill 5276 could be too broad, which may lead to undue restrictions on the free flow of data. On the other hand, the scope of protected data may be too limited if the “reasonable efforts” standard is too narrow. Contractual or other limitations on the re-identification of anonymized data also could be considered as a supplement to rights of privacy under the legislation. The GDPR suggests that “account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments” (GDPR, Recital 26), which may be an effective model. In the U.S., the Health Insurance Portability and

---


Unlike privacy legislation in other jurisdictions, Article 13 (§ 2) of Bill 5276 provides the competent body regulating anonymization standards and techniques with no direct reference to the standards or techniques employed in the anonymizing process. The Sections recommend that Bill 5276 be further clarified in this regard, with the GDPR and HIPAA approaches as a possible model.

5. The Written Consent Requirement of the Bills

The requirements to obtain informed consent from data subjects used to be the foundation for gathering, processing, and disclosure of personal information under EU privacy law. However, modern data processing requirements have moved towards a “legitimate interest” standard for processing. In the EU, the GDPR places increasing emphasis on legitimate interest for processing rather than consent as a basis for processing. Implicit, or opt-out, consent also is commonly used in online services and mobile applications.

In keeping with these norms, the Bills acknowledge the role of “lawful” or “legitimate interests” for processing data. Bill 330, Article 12 provides that “[h]andling of personal data may be performed …when required for fulfilling the legitimate interests of the person in charge of the handling or third parties to whom the data has been communicated.” Bill 5276, Article 7 also provides that treatment of personal data may be performed “when required for fulfilling the legitimate interest of the controller or a third party, unless the interests or fundamental rights and freedoms of the data subject prevail and require protection of personal data, especially if the data subject is a minor.” The Bills, however, also appear to rely extensively on requiring formal, written consent prior to processing of information. Article 12, Section I. of Bill 330 requires “free, specific and unequivocal and informed consent of the data subject,” and Article 7, Section I. of Bill 5276 similarly requires that the data subject give “free, informed and unequivocal consent.” Moreover, Article 12 of Bill 330 provides only limited exceptions to the requirement for obtaining explicit written consent.

Although consent is important, and the procedure specified in the Bills can be a useful mechanism for establishing a legal basis for processing, it should not be the only method for establishing a legal basis to process data. Requiring explicit written consent for all processing may actually undermine the goal of securing informed consent because consumers are likely to experience “consent fatigue” and may simply check “accept” to move through a transaction or signup without meaningfully reviewing options before providing consent.

In the United States, the Federal Trade Commission (“FTC”) has recognized that consent reasonably may be inferred from the context in which the data subject interacts with the data controller, and that affirmative express consent should be required only when the particular use of data would be unexpected by the consumer. As the FTC noted, “[c]ompanies do not need to provide choice before collecting and using consumer data for practices that are consistent with

4 See 45 C.F.R. §§ 164.514(b)(1) and 164.514(b)(2).

5 In comparison, see Directive 95/46/EC, Section II, Article 7 (allowing legal basis through mechanisms including: (a) consent; (b) compliance with a legal obligation; (c) protection of vital interests of the data subject; (d) public interest or official capacity; and (e) legitimate interests pursued by the controller (balanced against the privacy risk to individuals of processing)).
the context of the transaction, or the company’s relationship with the consumer, or are required or specifically authorized by law.”6 This concept captures the need to obtain consent where a consumer would not expect the specific processing at issue, but recognizes that modern digital life includes circumstances in which the need to obtain written consent at every turn is a burden on consumers and businesses alike.

The Sections suggest that eliminating reliance on implied or opt-out consent could negatively impact the online and mobile markets in critical ways. Most online advertising networks, both in Brazil and globally, rely on expressions of implied or opt-out consent as a basis to process that user’s personal data. In addition, online operators that provide goods and services use opt-out consent to process personal data once the initial, opt-in consent event has occurred. In certain situations, opt-out consent preserves the continuity of the user’s online experience by avoiding an intrusive consent mechanism each time an advertisement is served or other interaction occurs. For example, map applications require ongoing access to a user’s geolocation data. The user expects this and typically does not want to be prompted for consent each time the application collects such data. Rather, continued consent is implied, unless the user indicates otherwise. In addition, implied or opt-out consent does not require the user to take an affirmative action to signal consent, but rather recognizes that the user has consented to the practice. Requiring that a user affirmatively indicate his or her consent each time an interaction occurs may downgrade the user experience, a consequence that is recognized as a hindrance to the development of the digital ecosystem.

The Sections suggest that a “contextual” standard that defines the consent obligation based on the context and privacy expectations of the transaction is preferable to a uniform reliance on explicit written consent. Thus, opt-out consent may be appropriate when the collection and use of personal data are in line with the user’s privacy expectations and online interactions, while affirmative consent would be required only when the collection and use of a user’s data would be inconsistent with the context of the interaction. To effectuate this approach, the Sections suggest that the Bills include the concept of implied consent.

6. **Data Security**

   a. **“Constant” Updating of Security Measures**

   Both Bills address data security requirements for data holders/persons in charge of data; however, both also require that companies adopt “constantly updated” measures in their privacy and collection programs. The Sections resubmit that Bill 5276 adopt the previous recommendations and similarly recommend that Bill 330 adopt an “ongoing basis” standard. The “constant” and “continuous” standard could impose overly stringent and expensive requirements to comply with the plain language of the law, while not actually providing meaningful added protections.

   Bill 5276 changed some of its language from Article 42/45, but did not adopt the Sections’ recommendations. Article 6 of Bill 5276 provides that personal data handling activities observe security principles7 “through which constantly updated technical and

---


7 Bill 5276, Article 42 required.
administrative measures should be used in proportion to the nature of information handled and be capable of protecting personal data from unauthorized access and accidental or illegal situations involving destruction, loss, alteration, communication or diffusion.” The Sections recommend instead that security measures be periodically assessed and updated as necessary.

Bill 330, Article 29(I)(h) provides that the person in charge of the data must implement a privacy governance program that, among other things, may “be constantly updated based on information obtained from continuous monitoring and regular assessment” (emphasis added). The Sections suggest that it would be sufficient to adopt a program that assesses on an “ongoing” or “periodic” basis with updates “as necessary.”8 With recommended revisions, data holders must still improve safeguards in response to new threats and update frequently enough to protect subjects’ data.

b. Immediate Notification in Case of Data Breach

Both Bills address a controller’s notification requirements to the competent body in the event of a data breach. As data breaches continue to grow in magnitude and complexity, the Sections acknowledge that timely and accurate information regarding a breach is an essential part of protecting data subjects from harm, allowing parties to take swift measures to secure sensitive information, and prevent further harm from taking place. As the legislature recognizes, it is important that the competent body is promptly aware of new and evolving threats.

Article 47 of Bill 5276 provides that a controller must notify the competent body within a “reasonable time” of “the occurrence of any security incident that may lead to a material risk or damage for data subjects.” Article 24 of Bill 330, however, requires that the controller “immediately” notify the competent body of “any safety event that may cause damage to data subjects.”

The Sections’ previous comment recommended that Bill 5276 adopt a standard whereby controllers would be required to report security incidents “without unreasonable delay.” “Without unreasonable delay,” or within a “reasonable time,” is a more flexible standard that can help address some of the negative consequences of an immediate notice regime. In practice, “immediate” notice requirements can result in premature notice before the scope and extent of a breach can be fully known, which may not benefit consumers or regulators.

Under this standard, a controller can devote time and attention to adequate information gathering, rather than rush through a review—helpful in determining the true nature of the breach, gaining a more complete picture of cause and scope, and providing more accurate

---

8 Article 22 requires that the person in charge “adopt technical measures updated and compatible with international standards, as provided for in the regulations, with the nature of the data handled and the purpose of the handling.”
information for the competent body to determine next steps. Premature reporting fails to take into account the challenges a controller faces and creates disincentives for thorough investigation. Moreover, premature reporting may result in excessive reporting to both competent authorities and data subjects. Authorities’ resources would be strained managing events in which data were not actually compromised. And data subjects could experience reporting fatigue, rendering them unable to differentiate high- and low-risk threats.\(^9\)

To address the risk that a controller may delay reporting, the Sections further recommend adoption of Bill 5276’s requirement that reports include the reasons for delay in cases where notification did not take place immediately.

c. **Materiality of the Data Breach**

We reiterate the points made in the Sections’ previous comment. Article 24 of Bill 330 requires immediate notification of “any safety event that may cause damage to data subjects.” It is helpful that the language specifies that there must be a risk of damage to data subjects. To further clarify, however, the Sections recommend including that the risk of damage should be “material.” Like the immediate notice regime, lack of materiality can lead to excessive reporting to competent bodies, adding further unnecessary burdens and expense for all parties.

Article 48 in Bill 5276 and Article 24 of Bill 330 both require that controllers notify data subjects of the incident when there is a possibility of endangering the personal safety of data subjects or causing them harm, irrespective of the decisions that are made by the competent body after its evaluation of the incident.

Neither Bill requires materiality. The Sections submit that both Bills should require prompt notification where there is a possibility of “material” risk or harm. This requirement would again reduce the potential for unnecessary or excessive reporting.

7. **Cross-Border Data Transfers**

Under the current technological landscape, data are being transferred internationally on a daily basis. Automated processes in global enterprises have become a critical component to effectively and efficiently run cross-border operations. Global businesses that automate their processes likely transfer data across borders on a daily basis. Given the ease with which data can be transferred from one jurisdiction to another, the importance of providing clear provisions on the international transfers of data cannot be overstated. Any comprehensive privacy law must address its applicability to portable data and drafters should work with the international community to maintain consistency in this area.

The Sections restate that the Bills’ approach to international transfers is structurally sound and commends the Brazilian legislature for providing more clarity with the introduction of the “Controller and Operator” section. Providing a clear distinction between the controller and the operator is a critical component of compliance with data transfer norms. Each party must know its respective obligations when discussing the necessary transfer mechanisms and distributing obligations.

---

Equivalency Requirement. Both Bill 330 and Bill 5276 contained clauses permitting the personal data transfers to countries that maintain the same degree of data protection. Article 26 of Bill 330 sets forth this requirement by allowing transfers “to countries that afford the same degree of data protection provided for under this law.” This language was slightly amended in Article 33 of Bill 5276, which authorizes transfers “to countries that provide personal data protection equivalent to the level herein or higher.” The intent of these provisions is unchanged and the competent body will evaluate a foreign country’s level of data protection based on: (i) the general and sector rules under current law in the country of destination; (ii) the nature of the data; (iii) compliance with general principles for the protection of personal data set forth herein; (iv) the adoption of security measures set forth in regulations; and (v) other specific circumstances relating to the transfer.

Exceptions. Bill 5276 provides exceptions that permit data to be transferred to a country that does not, in the judgment of the competent body, provide an equivalent level of protection. The exceptions are: (i) international legal cooperation; (ii) protection of the data subject’s or third party’s life or physical safety; (iii) authorization of the transfer by the competent body; (iv) transfer arising from cooperation under international agreement; (v) public policies; or (vi) data subject consent when the data subject is advised of the risks involved and the international character of the transfer. This last exception is a departure from Bill 330. While there was an exception for data subject consent, the language was altered slightly from “properly informed” to “previously provided with specific information … and advised as to any risks involved.” The Sections commend the Brazil legislature for providing clarity on these requirements. These exceptions, however, will likely run into the same controversies that the EU regulations have experienced. The biggest concern arises where there is a need to rely on the “competent body,” which has the potential to result in severe administrative delays. The Sections respectfully suggest that it would be helpful to have a clearly defined and streamlined process that imposes fewer requirements on the competent body.

Privacy Shield and Other Transfer Mechanisms. Article 34 of Bill 5276, addresses specific authorizations if the “controller provides sufficient guarantees of compliance with the general principles of data protection and data subject rights.” This can be done by (i) contractual content approved by the competent body; (ii) standard contractual content; or (iii) global corporate rules in accordance with the regulations. These are important mechanisms that help streamline the process of transferring data, but they once again run the risk of process inefficiencies and delay — while waiting for the competent body’s analysis and approval.

The Sections respectfully suggest that the International Transfer of Data should incorporate an operational exception that would assist in expediting compliance and removing some of the large burden that Bill 5276 places on the competent body. An operational exception called the Privacy Shield is provided in the current EU-US data protection framework.

Utilizing this mechanism, enterprises can self-certify compliance with more stringent data protection requirements. This solution provides increased flexibility for the data processors and enforceable legal obligations that protect the data subject’s privacy. The new Privacy Shield requires clearer safeguards from U.S. authorities and contains a dedicated ombudsman to follow up on complaints or other inquiries from data subjects. The Sections once again stress the

---

10 For a description of that framework, see Privacy Shield, [https://www.privacyshield.gov/welcome](https://www.privacyshield.gov/welcome).

importance of having a self-regulation procedure to achieve compliance with applicable data privacy laws while increasing operational efficiency, especially given the increase in cloud-computing.  

8. **Big Data Issues**

“Big Data” specifically refers to the use of predictive algorithms to analyze massive data sets (volume) with real time data (velocity) of different types and from different sources (variety; collectively referred to as the “Three V’s”). Two other “V’s” also play a role in big data analytics: variability/value (i.e. the change in other characteristics) and veracity (i.e. the integrity or trustworthiness of data). Predictive algorithms seek out probabilistic connections between data elements.

There are many benefits to society of big-data analytics, particularly in healthcare and education (e.g., to identify and provide early intervention to “at risk” students). Big data analytics can be crucial to optimize urban transportation and management and to devise strategies for emergency preparedness for disaster response and city management. At the same time, concerns have been raised about whether data analytics may be used in a non-transparent way to categorize consumers in ways that prejudice them. Careless collection and analysis of data can generate conclusions about persons that inadvertently express or reinforce inappropriate biases.

a. **Defining Automated “Decision Making” to Permit Lawful, Beneficial and Innovative Data Uses**

As noted above, analytics can be helpful in many instances such as health, education, security, and urban planning, with likely many other beneficial uses not yet discovered. The law should not preclude lawful and beneficial automated decision making. Any restrictions should be focused on the misuse of analytics.

There are threshold issues relating to (i) what are automated decisions, and (ii) who is making them. For example, if a person is identified as a potential target for advertising, is that a “decision”? And if the algorithm for identifying that individual is developed by entity A, sold by entity B, and used by entity C, who has made that decision?

**There should be a materiality threshold on restricting automated decision making.** Bill 5276, Article 20 applies broadly to “decisions made solely on the basis of automated handling of personal data affecting their interests, including decisions used to define their profile or assess aspects of their personality” (emphasis added). Bill 330, Article 10 would ban automated decision making if an individual is “excluded, harmed or in any way affected in their legal sphere by decisions based solely on automated handling of data intended to evaluate their profile” (emphasis added). The Sections note that the European Union, in the recently enacted GDPR, defines the universe of automated decision making subject to its rule in Article 22(1) as “a decision based solely on automated processing, including profiling, which produces legal effects

---

12 The Sections recognize that Privacy Shield is the subject of debate within the EU, but believe that this new mechanism will overcome the shortfalls that resulted in invalidation of the Safe Harbor framework.
concerning him or her or similarly significantly affects him or her” (emphasis added). We suggest a materiality limitation in line with the GDPR approach.13

b. Permitting Automated Decision Making Based On Legitimate Interest, Subjecting Automated Decision Making to a Challenge Right Based on Breach of the Data Subject’s Fundamental Rights, and Related Points

The Sections encourage that the use of automated decision making should be permitted in the first instance without express consent as long as there is a “legitimate interest.” Both Bills recognize “legitimate interest” as an exception to the requirement of express consent. Legitimate interest is defined in both Bills as the “legitimate interest of the controller or a third party” in Bill 5276 Article 7(IX) “unless the interests or fundamental rights and freedoms of the data subject prevail and require protection of personal data, especially if the data subject is a minor” and in Bill 330 Article 12 (VII) “as long as said interests do not prevail over the interests or rights and basic liberties of the data subject” (emphasis added). Bill 330, Article 10 (§1) provides that “[t]he decisions … shall be permitted upon entering into or performing a contract agreed upon by the individual” subject to the right to challenge discussed below. This language suggests that automated decision making may only be permitted by contract. As noted above, the Sections respectfully suggest that automated decision making should be permitted even without a contract if justified by legitimate interest.

The Sections suggest that the right to challenge automated decision making and obtain manual intervention should be based on a specific claim of breach of a data subject’s “interests or fundamental rights and freedoms.” Only Bill 330 (Article 10) addressed this right to challenge, providing that “[t]he decisions … shall be permitted upon entering into or performing a contract agreed upon by the individual, provided that measures to ensure the possibility of challenge, immediate human intervention, and other legitimate interests of the individual are guaranteed” and that “[t]he decisions … may always be challenged by the data subject, the right to obtain reasoned human decision after the challenge being ensured” (emphasis added). As a point of comparison, the right to object to profiling under the GDPR has to be based, “on grounds relating to his or her particular situation” (emphasis added). The right to challenge in the Bills is unqualified and could lead to misuse. The Sections recommend that the right to challenge should be aligned with the reason for permitting such challenges—to protect the fundamental rights of the data subject. Additionally, we recommend that the scope of manual intervention (“the reasoned human decision”) should, in turn, be dependent on the legitimate bases asserted for challenging the automated decision.

The Sections urge that disclosure of the “logic” underlying the algorithms should be subject to the protection of intellectual property rights. The protection of intellectual property

13 In addition, the Sections believe that the health care and protection of life and physical safety exceptions are too narrow. Both Bills specifically exclude from the definition of processing “[t]o protect the life or physical safety of the data subject or a third party” and “[f]or healthcare procedures conducted by healthcare professionals or public health authorities.” Bill 5276 being the more explicit. That articulation may be too narrow as there are other beneficial uses. For comparison purposes, the GDPR defines “profiling” specifically in terms of areas of concerns, limited to “the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements” (emphasis added).
rights necessary for innovation is recognized only in Bill 5276 Article 20, which provides that “[w]henever so requested, the controller shall provide clear and adequate information in relation to criteria and procedures used for automated decisions while keeping commercial and industrial secrets.” The Sections recommend that this protection be included in the final legislation.

The Sections submit that use of publicly available data should not be restricted. Bill 5276 Article 7.IX (§4) provides that “[p]ublicly accessible personal data must be handled in accordance herewith, having regard to the purpose for which the data were provided and the good-faith and public interests for doing so.” The Sections believe that these terms are too restrictive. The value of big data to some extent lies in the identification of unanticipated, but valid, correlations between data elements. The Sections encourage that certainly insofar as the data already legitimately in the public domain, their use should be permitted.

9. Rights of Data Subjects under the Bills

a. Right to Be Forgotten

Bill 330, Article 6, Sections VII and IX, defines basic rights of the data subject to include protections that may establish a “right to be forgotten.” Article 6, Section VII, provides that a basic right of data subjects is “permanent deletion, upon their request and upon the termination of the relationship between the parties, of their personal data in any databases, except for other legal reasons that may affect the custody of data.” Article 6, Section IX provides that another basic right of data subjects is “self-determination with regard to the handling of their data, including confirmation of personal data handling, access to data, correction to untruthful, inaccurate, incomplete or outdated personal data at no cost, and cancellation of unnecessary and excessive data or data not handled in accordance with this law.” Bill 5276, Article 18, Section III, defines the rights of the data subject to include “correction of incomplete, inaccurate or outdated data.”

The Sections recognize and acknowledge the desire to maintain data subjects’ control over the continued use of their information. But data controllers may have legitimate and compelling reasons to retain personal data, a need we suggest should be balanced with an individual’s right to be forgotten. Describing the right to be forgotten in absolute terms could have unintended consequences, including: (1) denial of an individual’s ability to enforce legal rights; (2) facilitating illegal activity; (3) endangering health and safety; and (4) impeding the advancement of legal defenses. The Sections advocate that the “right to be forgotten” should be implemented as a set of principles recognizing data subjects’ ability to cause the deletion of their personal information from digital memory where appropriate, rather than as an overriding personal right that may conflict with the need of some data controllers to maintain that data in certain circumstances.14

---

14 The GDPR identifies the following lawful purposes for further retention: “for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.” Regulation 2016/679, 2016 O.J. (L 119), Recital 65.
b. Data Portability Right

Bill 5276, Article 18, defines the rights of data subjects to include “portability upon request of their personal data to another service provider or product.” The Sections recognize and acknowledge the desire to maintain data subjects’ control over the downstream use of their information. But unlike privacy legislation in other jurisdictions, such as GDPR, Article 20,\(^{15}\) there is no mention of parameters for data that must be portable to provide guidance and appropriate limits. The Sections recommend providing further clarification regarding the parameters of data that must be portable.

10. Enforcement and Implementation

a. Conflicting Legal Obligations

The Sections recommend that the Bills expressly acknowledge that conflicting legal obligations may in some cases justify exceptions to the Bills’ requirements, to the extent necessary for data controllers to discharge those obligations. Bill 330, Article 35, states that the rights provided in this law do not displace those arising from international treaties or conventions to which Brazil is a signatory, from internal legislation, and from regulations issued by the competent administrative authorities. Although this language indicates that the rights contained in Bill 330 are not exclusive of rights contained in other laws of the country, the Sections recommend that the Bills also provide guidance on when the rights and obligations contained in the Bills may be in conflict with other laws and regulations in Brazil.

For example, the GDPR contains three provisions that specifically circumscribe its reach so as to not conflict with other European and national laws.\(^ {16}\) Most significantly, the GDPR explicitly states in Article 96 that international agreements that involve the transfer of personal data to third countries or international organizations, that were concluded by Member States prior to May 24, 2016, and that comply with Union law then applicable, remain in force until amended, replaced, or revoked.\(^ {17}\) The Sections recommend that the Bills similarly include explicit provisions on what law should take precedence when there is a conflict between a provision in the Bills and other laws and regulations in Brazil.

b. Joint and Several Liability

The Bills provide for joint and several liability between data transferors and data transferees in a number of provisions. Bill 330, Article 20, Paragraph 2, and Article 28, Paragraph 3 hold jointly and severally liable “all those who have access to the data,” regardless of their fault. In Article 34, Bill 330 also holds jointly and severally liable member companies or entities of an economic group, when at least one member or entity violates the law. Similar provisions in Bill 5276, Article 34, Paragraph 1, and Article 35, hold transferor and transferee

---

\(^{15}\) Article 20 of the GDPR grants data subjects: (1) the right to receive the personal data provided by them, in a structured, commonly-used and machine-readable format if the data was provided on the basis of consent or contract; and (2) the right to have the personal data transmitted directly from one controller to the other when technically feasible.

\(^{16}\) Regulation 2016/679, 2016 O.J. (L 119) 1, 32, 86, 87.

\(^{17}\) Id. at 87.
jointly and severally liable regardless of their fault and their locations. Bill 5276, Article 44, specifically holds transferees jointly liable with transferors for any damage caused.18

The Sections are concerned that these joint and several liability provisions are inappropriate because they conflict with underlying tort law concepts, and accordingly would result in unjust treatment of innocent data transferors and transferees. In tort law, joint and several liability typically applies where there are two or more actors who both breach a duty of care to a third person, and either it cannot be determined which one caused the damage to the third person, or both caused the damage. Consistent with tort law, the GDPR includes only very narrow joint and several liability for data transferors and data transferees, limited to instances in which both caused damage to the data subject.19

The Sections recommend that the Bills exclude joint and several liability, or at least narrowly circumscribe its application to instances in which two or more parties both caused damage to the data subject. The Bills’ joint and several liability provisions conflict with tort law concepts in several respects. First, when one party alone — be it the data transferor or the data transferee — breaches its duty to the data subject, there is no justification for holding another party liable who breached no duty to the data subject. Second, in the highly unlikely case that both data transferor and data transferee breached their duty to the data subject, it is even less likely that the data subject will not be able to determine which party caused the damage, or that both breaches will be inseparable causes of the damage. The Bills’ provisions as written could subject innocent parties to full liability for another party’s breach.

c. Penalties

In addition to requiring persons who inappropriately handle data to compensate those damaged by their actions, the Bills also levy penalties in excess of those damages. In Bill 330, Article 31 subjects persons who have inappropriately handled data to a fine of up to 5 percent of the net revenues of the economic group in Brazil for the latest fiscal year. Bill 5276, in Article 52 (§2), also establishes a punitive system whereby a company may be subject to several sanctions for a single breach.

The Bills’ penalties should be effective, proportionate, and have a deterrent effect.20 Five percent of net revenues generated in Brazil in the latest fiscal year could be disproportionate and excessively punitive. Such a penalty could discourage companies from reporting potential violations or cooperating with regulators to solve problems, particularly in the data security area. Even the GDPR, which provides for significant fines, has carefully calibrated criteria to determine when higher fines are appropriate.21

The Sections recommend that the Bills calculate the penalty in a gradated manner under the GDPR model, with appropriate considerations for whether the full penalty is appropriate for a particular potential violation.

18 Bill 5276, Article 44 also contains a narrow carve-out, exempting data handling carried out in the exercise of duties under Law 12527 of 2011 from joint and several liability.
19 Regulation 2016/679, 2016 O.J. (L 119) at 81.
20 Id. at 83-84.
21 Id. at 83.
d. Transition Period

The Sections suggest that the vacatio legis or transition periods of each Bill be longer than the period originally suggested. Bill 330, Article 37, states that the law will come into force and effect 120 days following its official publication. Bill 5276, Article 56, states that the law will come into effect 180 days after the date of its publication. These two transition periods contrast starkly with the GDPR, for which the transition period is a full two years from the date of publication.22 The Sections recommend that the Bills employ a similar period. While data controllers would struggle to come into compliance in just four or six months from the date of the Bills’ publication, a longer period would enable data controllers to understand better and comply fully with the new data protection regime. A transition period of at least one year would provide more time for the Federal Government to assemble a competent body to oversee the data protection regulations, and for that body to establish administration and implementation structures to enforce the new regulations.23

The Sections also recommend the implementation of a transition rule on renewal of consent, similar to the GDPR under which:

[p]rocessing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorizations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

IV. Conclusion

The Sections appreciate the opportunity to comment on the Bills, and commend the Brazilian government for its open and transparent process. If the Sections can clarify any of the matters discussed herein or answer any questions, we would be pleased to do so.

22 Id. at 87.
23 Bill 5276, Article 56, states that the competent body shall determine the progressive adequacy requirements for treatment of an existing database. The Sections urge clarification on this point as it is vaguely open-ended.