Centre for Information Policy Leadership
Hunton & Williams LLP

6 April 2017

DISCUSSION POINTS
BRAZIL PROPOSED DATA PROTECTION LEGISLATION
330/2013 – SENATE BILL

The following points are CIPL's comments on certain key issues relating to Brazil's draft Senate bill 330/2013. Please note that our comments are based on English translations of the text. It is possible that, as a result, we may have misunderstood some particular intent or nuance on a particular issue, in which case, please disregard our comment on that issue.

1. General comments

By way of general comment, CIPL believes that the current draft includes several significant improvements over earlier drafts. For example, we welcome the inclusion of the "legitimate interest" ground of processing, the inclusion of risk assessment and, thus, a risk-based approach in the provision on "privacy management programs", and a broad range of cross-border transfer mechanisms, among other items.

Over the past few years, a global "data and digital revolution" has drastically changed the landscape to which data privacy laws apply. We now live in a new "digital age" that is based on and driven by big data, the Internet of Things (IoT), Artificial Intelligence (AI) and machine learning. Everything is data and data is everywhere. Data flows around the globe in ever-increasing quantity and is used in ever increasing and complex ways. This presents a new reality that has to be taken into account when devising new privacy and data protection laws that are fit for the new information age. Brazil currently has a unique opportunity to create a law that can meet the needs of this digital age, taking into account the experiences, mistakes and successes of other privacy regimes around the world. Most if not all of these legacy privacy regimes were devised prior to the digital age and are now also faced with the need to modernize.

In that connection, it is important to avoid creating laws that will become obsolete with the next technological advancement or whose total impact is not fully understood at the time of drafting and that, therefore, may have unintended consequences for legitimate and beneficial data uses. Naturally, it is the organisations who will have to comply with these provisions that are in the best position to foresee such potential consequences. Thus, we strongly recommend that as part of multistakeholder consultations, these organisations be extensively consulted on the details of any final provisions.

To be able to meet the demands of this new digital age and be future -proof, we believe that a data privacy law for Brazil must have the following key characteristics:

1. **Be clear and easy to understand, apply and enforce**. This law has a wide scope of application and would apply to all personal data (of citizens, customers, employees, business contacts) and cover all industry sectors and commercial enterprises of all sizes, including sectors with no data protection experience and small businesses with no expertise

or ability to hire data protection officers to help them comply. It is essential that the requirements be simple, easy to comprehend and implement across the board.

2. **Follow a principles-based approach:** Rather than include too many specific and detailed requirements, high-level principles and "goals" will allow organisations to apply these principles flexibly with the help of appropriate benefits/risk analyses that will determine the specific appropriate data protection measures for a given context, particularly as technology and business practices change and individuals' expectations evolve.

3. **Include a risk-based approach:** This means that organisations should be required to understand the risks and harms to individuals of any data processing and data use, as well as benefits of processing, and are able to calibrate compliance based on potential risks and harms. In that way, they can concentrate their compliance efforts, mitigation actions and accountability (good practices) on areas that may cause risks and harms. Equally, they should not spend too much effort on areas that do not create risks and harms to individuals, such as in the B2B data processing context, or other common and everyday uses of data.

4. **Remain technologically neutral:** (e.g., on issues such as data security) so that the law can adapt to technological changes and remain relevant.

5. **Provide for varied legal basis for processing and data transfers:** The law should include a range of grounds for processing, ranging from consent to legitimate interest, each of which can be applied pragmatically in appropriate contexts to enable the full range of beneficial data uses in the modern information age while also protecting the individual. The law must also provide for a broad range of cross-border transfer mechanisms that mirror and are able to work with all other international transfer mechanisms to enable the seamless flow of data around the globe that is essential both to a modern economy and the use of data for commercial purposes and for societal progress.

We believe that much of this is already accomplished by the current draft. However, the more detailed comments below on some of the key provisions in the draft may further improve this law consistent with these high-level concepts.

2. Controller/Processor Distinction and Scope of Jurisdiction (Article 2)

Overarching message: The law should clarify its respective application to controllers (person in charge) and processors (operator), with the application to processors being limited to the security provisions and privacy governance programs (Article 29). In addition, the law should make clear that Brazilian privacy law does not apply to the processing of foreign data by Brazilian processors on behalf of foreign/non-Brazilian controllers. In general, the law should apply to organisations (controllers or processors) established in Brazil, irrespective of where they process the data. Further, processing of personal data of Brazilians who make online purchases from non-Brazilian domains/websites (e.g. .com rather than .br), should not be subject to this law.

- Imposing Brazilian privacy law on foreign controllers would create significant impediments for the Brazilian IT service industry as well as other processors in Brazil that provide services to global clients. Brazilian processors that process data on behalf of their foreign clients must be able to meet the requirements of relevant foreign law that applied to the data at the point of collection. For example, if a Brazilian processor processes data on behalf of a Belgian controller, the Brazilian processor must be able to apply the relevant Belgian law to such data – not Brazilian law.

- As a general matter, the law should extend only to those controllers located outside of Brazil that specifically direct their services to Brazilian residents and purposefully collect personal data of Brazilian citizens. Thus, we believe that foreign controllers generally should not be subject to Brazil's privacy law if Brazilian consumers purchase goods from non-Brazilian domains/websites such as .com (rather than .br).

3. Anonymisation and Anonymised Data (Articles 2 and 3)

Overarching message*:* Legislation should promote the use of anonymisation as a way to reduce risk to individuals. Companies need certainty that anonymised data is not subject to this law, and that data is considered anonymised when re-identification can only be accomplished through extraordinary efforts.

- The draft bill clearly recognizes the importance of anonymisation, and appropriately excludes such data from this law. Processing anonymised personal data enables a broad range of benefits, such as big data analytics for purposes of scientific research and product improvement and development. The draft law acknowledges this, by clearly stating that it does not apply to "anonymised and dissociated data."

- The provisions provide that anonymous data is data that "cannot" be identified with "reasonable" technical means. We suggest that the bill clarify the standard for "reasonable" technical means to the effect that whenever "extraordinary" efforts are necessary to re-identify anonymous data, such data would not be covered by the law. In addition, we suggest that data should still be deemed anonymous for purposes of this law even where it could be re-identified through "reasonable" means, if the anonymisation is coupled with additional procedural, administrative and legal protections against de-anonymisation or re-identification. Thus, we recommend that the draft law also incorporate procedural, administrative and legal protections, such as enforceable contractual commitments with third parties and service providers not to re-identify anonymised data, as well as legal prohibitions not to do. This will further help to ensure that anonymised data may be recognized as such and excluded from the law.

- We acknowledge and appreciate that anonymisation that could be reversed poses a risk to the data subjects. On the other hand, companies should be encouraged to attempt to anonymise data because it reduces the risk to data subjects. Subjecting companies to an unclear or difficult to meet standard of whether an anonymisation technique is "reasonably" be reversible or

meets the necessary level of anonymisation to take the data outside of the application of this law provides little incentives to organisations to anonymise the data and has little practical utility.

- Finally, because sometimes re-identification of anonymous data is necessary to provide certain services, for example in the health and medical arena, it would be useful to include criteria for when such re-identification of personal data is permissible.

4. Legitimate Interest and Consent (Article 12)

Overarching message: While consent remains important in some circumstances, the emerging data environment and technologies – particularly big data, the IoT and analytic processing – requires increased reliance on legitimate interests as a basis for processing.

- CIPL is encouraged by the inclusion of legitimate interests as a legal basis for processing of data. In many contexts, legitimate interest is in many cases the more "accountable" basis for processing and provides greater protections for individuals because it requires an assessment and balancing of risks and benefits in each instance as well as the implementation of context-specific mitigations.

- However, as written, the legitimate interest provision limits the application of this ground for processing by excluding the interests of society. The current draft includes a requirement that only the interests of "third parties to whom the data has been communicated" may be considered. Typical legitimate interest clauses, such as the EU General Data Protection Regulation (GDPR), do not include this communication requirement. This additional phrase precludes an interpretation that the legitimate interest ground for processing also protects the legitimate interest of society, which is precisely one of the key considerations in connection with many types of modern processing and big data analytics that enable societal progress. We strongly encourage deletion of that phrase.

- As to consent, we believe that in cases where express consent is not required (i.e. in connection with non-sensitive data), valid ways to consent should include opt-out and implicit consent to ensure individuals are not overburdened by constant consent requirements in the digital world. This should be made more clear in the law.

5. Sensitive Data (Article 15)

Overarching message*:* Care must be taken to ensure that consent provisions related to sensitive data not become so restrictive that they preclude the use of that data – with appropriate safeguards – for beneficial uses.

- CIPL is concerned that the consent provisions related to sensitive data may be too restrictive and not reflect the realities of contemporary data use.

- Requiring express consent for sensitive data processing will preclude a large number of beneficial uses of data (including uses that have not only commercial value but would benefit society), where the controller is not in a position to obtain consent or where consent is denied for no good reason in cases where there is no harm, for example. A more clear and pragmatic anonymisation provision along the lines described may solve much of this problem. In addition, it may be helpful to allow for legitimate interest-based processing of sensitive data in contexts where obtaining consent would be impossible or impracticable.

- We also suggest that the research exemption be clarified to explicitly include research that is "associated" with commercial activities. Currently, a great deal of research that benefits society is conducted by commercial entities. Organisations should be able to use sensitive data responsibly both for commercial purposes and broader purposes that benefit society if the data is handled accountably and the is no or very low risk of harm

6. Data Breach Notification (Article 24)

Overarching message: "Immediate" or "prompt" notification of the breach to the competent authority and/or individuals is unrealistic and potentially harmful.

- The draft requires notification to the authority and/or individuals immediately or promptly. That is unrealistic and potentially counterproductive. Experience shows that companies need time to establish the facts and nature of the breach, what data has been implicated, and what impact, risks and harms can arise from the breach. It takes time to undertake such forensic and legal analysis and there is no point notifying and burdening people and authorities until and unless facts are known and the risks and potential harms are assessed. In addition, in some circumstances it is important not to disclose to individuals and publicly that a breach as occurred pending a non-public criminal or other type of investigation.

- CIPL recommend that any breach notification requirements be refined to include that notification occur immediately after the facts and the nature of the breach have been established, and only after the potential impact, risks and harms for individuals have been established (the latter point appears already to be in the current draft only in respect of the duty to notify individuals).

- Encryption is not an exception under the draft. Hence even where the data or a device was encrypted the breach must be notified. There should be a higher bar for triggering a breach notification requirement for encrypted data. If the risk assessment after the breach concludes that the data was sufficiently encrypted and that there is no risk to individuals, there should be no requirement to notify the authority or individuals.

- Requirements that companies should disclose the nature of the security measures taken should be either eliminated or significantly narrowed to include only the general nature of the security

measures taken. Disclosing too much information about security can compromise the efforts of professionals to remediate breaches and unnecessarily expose systems to compromise by bad actors.

7. Security (Article 25)

Overarching message: Specific security requirements cannot be set by legislation, but must remain future-proof, flexible and context-specific. Organisations should determine appropriate security measures based on standards, state of the art measures, cost, nature of the data and the risks involved.

- It is counterproductive to require that security measures be determined by laws or regulations, which immediately makes them outdated, given that the laws lag behind the technology and the development of technical standards. Determination of specific security measures is best left to organisations based on standards, state of the art, cost of measures, the sensitivity of data, and risks.

- It is best for data privacy laws to include a general security requirement to implement appropriate measures to protect data from loss, destruction, unauthorised access and other forms of unlawful processing (like in the EU GDPR). This leaves it to the organisations to determine what are appropriate measures to protect data from unauthorized access, loss, destruction, disclosures and processing in any given context, based on criteria mentioned above.

- We note that the same concerns exists in relation to sensitive data in Art. 18, sole paragraph, which currently appears to state that the specific security measures for sensitive data will be prescribed by law.

8. International Transfer of Data (Article 26)

Overarching message: CIPL welcomes the draft law's approach to cross-border data transfers to the extent it provides for a broad spectrum of mechanisms that can be used to legitimize transfers of personal data to countries that do not have similar levels of protection and to the extent these mechanisms can work together with similar mechanisms in other countries.

- In particular, we welcome the incorporation of widely accepted concepts of "standard contractual clauses" and "global corporate standards" or "global corporate rules" (known in Europe as "Binding Corporate Rules" or "BCRs"). These would position Brazil for data transfers with Europe and other countries that recognize these European cross-border transfer mechanisms.

- However, standard contractual clauses and binding corporate rules have limitations – the former are not flexible and can result in undue complexity and the latter are limited to transfers within a corporate group under the current Senate draft and lack scalability as they need to be

approved by the competent authority. (After the new EU General Data Protection Regulation (GDPR) takes effect, BCR possibly may also be used across and between corporate groups.)

- Therefore, while we strongly support the inclusion of these options, we encourage Brazil to work with experts, including CIPL, to improve on them and to make them more practical and scalable for widespread use by companies of all sizes.

- Moreover, we believe that the menu of choices available to companies should be broadened. Given that modern data flows and economic activity are global, we encourage inclusion of mechanisms such as privacy marks, seals, and organisational codes of conduct that are certified by appropriate third parties or a competent authority. These mechanisms are being adopted across the globe. One example is the APEC Cross-Border Privacy Rule (CBPR) system, developed by the APEC forum. Another example are EU Certifications under the EU GDPR. We believe it is important that data transfer mechanisms should allow for transfers not only within a global corporate group, but also between unaffiliated companies. Internationally recognized marks, seals and codes of conduct support this kind of transfer.

- Indeed, with respect to the requirement in the draft that the "competent body" authorize these global corporate standards or rules, we suggest that this requirement be modified to allow recognized certification bodies to authorize such standards or rules, similar to the role of Accountability Agents in the APEC CBPR system to avoid approval bottlenecks within this competent body.

- It is worth noting that APEC and the EU have begun to explore ways to streamline the CBPR/BCR certification and approval processes where companies seek "dual certification" under both systems. They are also exploring how to make the new EU GDPR Certifications compatible and interoperable with the CBPR. Thus, CIPL recommends that any Brazilian counterparts to these mechanisms be designed so that they too are "interoperable" with these and other similar cross-border transfer schemes to ensure that companies that have certified, or received approval under a non-Brazilian scheme can leverage that approval in Brazil and vice versa.

9. Privacy Governance Programs – Accountability (Article 29)

Overarching message: CIPL strongly supports the inclusion of this provision requiring comprehensive organisational privacy management programs that ensure compliance, reflect the structure of the organisation and the nature of its processing activities and that incorporate risk assessment and risk management as well as the ability to demonstrate compliance as a core element of such privacy governance programs. In addition, there should be specific incentives for organisations, both controllers and processors, to implement privacy management programs, such as a mitigation in enforcement and determination of penalties.

- To strengthen and clarify the inclusion of risk assessment in such programs, it might be clarified that, in addition to considering the risk to individuals from data processing, risk assessments must take into account the potential countervailing benefits of processing.

- The examples of the elements of privacy governance program should also include complaint handling procedures. To avoid overburdening the competent authority and/or the courts, it is important (and possible) that most complaints by individuals be addressed initially at the company level.

- The provision might also establish incentives for companies to formulate or adopt such governance programs, such as the ability to engage in more data processing, or to be able to share data, or as a mitigation in oversight and enforcement by a competent body. For example, in the case of an enforcement proceeding, companies that adopt and adhere to such programs, and can demonstrate good faith efforts to comply, might be subject to less enforcement and reduced penalties in the event of a violation. This is already a recognized practice with many data protection and enforcement authorities in different countries. This can be specifically added or made more clear in the Article 32 list of factors to take into account when imposing penalties.

- The provision should clarify that such privacy governance programs could be established by way of a certification or code of conduct and thus could also serve as recognized cross-border transfer mechanism, as described above on the use of certifications and codes of conduct as cross-border data transfer mechanism. (See for example the EU GDPR's use of certifications and codes of conduct as transfer mechanisms.)

- To the extent that rules, certification or codes of conduct are intended to serve as cross-border data transfer mechanisms, they should be devised in a way that allows them to be substantively and procedurally interoperable with similar schemes in other countries to enable cross-border solutions for companies and avoid constant re-certification of companies under similar standards.

10. Effective Date and Prospective Application (Article 56)

Overarching message: We believe that 120 days is insufficient time for covered entities to implement the new requirements. We recommend a three-year implementation period. Further, we strongly recommend that this law be clarified to have prospective rather than retroactive application to personal data that has been collected prior to its effective date.

- To become compliant, companies will need to become familiar with the provisions of the law, understand how it may be interpreted by regulators and practically applied, and take appropriate measures internally. This is particularly difficult where no previous comprehensive privacy law has existed.

- A reasonable timeframe would be at least three years. The EU GDPR provides for two years, and we can already see one year into the implementation phase that organisations will not be completely ready by May 2018.

- Experience shows that it takes a long time to ensure that old legacy IT systems and existing uses of data are fully brought in compliance with new rules. As organisations struggle to apply the new requirements to existing data and processing, they lose important time to ensure their new systems, data processing and technologies comply with the law.

- Thus, there the law should also not apply retroactively but only prospectively. It may be helpful to state that the existing data processing and use of data should be brought in compliance with the new law as and when the data are used for new purposes from the time of entry into force of the new law

Competent Body

Overarching message: A competent and independent data protection body or authority is critical to the successful implementation of data protection legislation in Brazil.

- We are concerned that while the draft bill refers to a "competent body," no specific provision is made for one in the text. The draft law's many provisions cannot be implemented without the "competent body" referenced throughout, yet the draft law does not address the creation of this authority.

- The experience with other data privacy laws and oversight around the world demonstrates that for this law to be effective, a single independent data protection and privacy enforcement authority is essential and should be created simultaneously with the draft law. To ensure consistency in interpretation and enforcement of the law, it is important that there be a single national competent authority rather than multiple competent authorities.

- National data protection supervisory authorities and privacy enforcement authorities play an important role in oversight, application, interpretation, education and enforcement concerning national data privacy law. Much more so than courts, they have the necessary expertise to interpret privacy law with the nuance and flexibility appropriate to the circumstance. As such, they occupy the important dual role of protecting privacy and enabling beneficial data uses, and, thereby, the digital age. They also have an important role to play as ombudsman in resolving complaints from individuals. Finally, they are indispensable to ensure a more harmonized and consistent approach to data privacy regulation and enforcement across borders. National data protection and privacy enforcement authorities work closely with each other through regional and international organisations such as the International Conference of Data Protection and Privacy Commissioners, the Asia Pacific Privacy Authorities (APPA), the Ibero-American Data Protection Network (RIPD), the APEC Cross-border Privacy Enforcement Arrangement (CPEA), and the Global Privacy Enforcement Network (GPEN). It is vitally important that Brazil be

represented in these organisations through a national privacy authority.

If you would like to discuss any of these issues further or require additional information, please contact Bojana Bellamy, bbellamy@hunton.com or Markus Heyder, mheyder@hunton.com