Centre for Information Policy Leadership
Hunton & Williams LLP

Comments of the Centre for Information Policy Leadership on Brazil's Revised Draft Privacy Law

The Centre for Information Policy Leadership (CIPL)[1] hereby submits comments on Brazil's revised draft privacy law (draft bill providing for the processing of personal data to guarantee the free development of the natural person's personality and dignity) released in October 2015.

In April 2015, CIPL had submitted comments[2] on the first draft of this bill, which was released in January 2015. We greatly appreciate the opportunity to follow up on our earlier comments with a few additional observations on the new draft.

Since the release of the first draft, we not only have provided the above-referenced written input into Brazil's process to develop a comprehensive privacy law, but also have talked with many key Brazilian stakeholders, including a number of policymakers and legislators involved in the development of this important law, as well as representatives from industry, civil society and academia. We have engaged both through delegation meetings with relevant individuals and a global privacy conference we co-hosted in Brasilia in October 2015 together with the Instituto Brasiliense de Direito Público. We very much appreciated the level of interest and receptiveness to our ideas that our Brazilian interlocutors have shown to us at all times.

We preface our further comments and observations below by commending the drafters for the many improvements that are evident in the revised draft bill. These include the inclusion of the concept of "legitimate interest" as a basis for legitimizing data processing, the more flexible definition and application of "consent," the inclusion of concepts of privacy risk management in "best practices," the ability of industry to use data for research purposes, the effort to devise an appropriate "anonymization" standard to take personal data outside the scope of this law, and other features. All of these will contribute to Brazil's producing a privacy law that will ultimately be appropriate for the modern data-driven economy and society and capable of enabling both effective privacy protections and innovation.

---

[1] CIPL is a global privacy and security think tank in the law firm of Hunton & Williams, established over 12 years ago. It is supported by approximately 38 member companies that are leaders in key sectors of the global economy. CIPL provides thought leadership and expertise on global privacy and security policy issues, working with privacy officers, regulators and external experts to develop best practices to ensure effective privacy protection and information management in the modern information age. For more information, please see the Centre's website at http://www.informationpolicycentre.com/. Nothing in this comment should be construed as representing the views of any individual Centre member or of the law firm of Hunton & Williams LLP.

[2] Comments available at:
https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Comments_Centre_for_Information_Policy_Leadership_Brazil_draft_law.pdf; and
https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Comentarios_do_Centre_for_Information_Policy_Leadership_Anteprojeto_de_lei_do_Brasil.pdf.

However, to achieve that goal, we believe that a few areas require further clarification and refinement. We will try to keep our suggestions on these points brief, referring you, in part, to our earlier comments where they already addressed the issue, and, otherwise, inviting you to seek further clarification from us where necessary. Please also note that our comments are based on a combination of various and sometimes divergent English translations of the Portuguese text, which may have resulted in some misunderstanding of the actual intent or meaning in some contexts.

I. Further Comments

Legitimate Interest

We welcome the inclusion of "legitimate interest" as a basis for processing among several alternatives that also include consent. We view this as a significant step toward enabling modern information uses, where consent is not always practicable or possible.

However, we suggest a couple of clarifications. Article 10(1) seems to provide that in applying the legitimate interest standard, one must consider the "legitimate expectations" of the data subject pursuant to Article 6(II), which provides that all processing (not just legitimate interest processing) must be compatible with the legitimate expectations of the data subject.

One of the values of legitimate interest processing is that it enables further processing for purposes that previously were unknown, unimagined and unexpected, such as where data was collected for one purpose but has now been discovered to facilitate a different purpose. If the "legitimate expectations" of the data subject at the time of original collection are the test for whether processing for the new purpose may go forward, then legitimate interest-based processing will neither serve its purpose nor add anything new.

The protection of the data subject in the context of legitimate interest-based processing results from the fact that the business interests at stake must be weighed against the potential harms to the individuals' fundamental rights and freedoms, as the draft law already correctly states. In light of this, it is not clear why the additional "reasonable expectations" requirement is needed and, in fact, it seems to undermine the legitimate interest basis for processing. We therefore recommend that the final version of the law clarify this point and exclude "legitimate expectations" from the test for "legitimate interest." Thus, Article 10 might be amended to read as follows: "Processing based on the legitimate interest of the data controller is valid if the stated legitimate interest is not outweighed by harm to the rights and freedoms of the individual, relates to a concrete situation and the processing is necessary for the intended purpose."

Consent

In the revised draft, consent apparently must be "express" only in connection with the processing of sensitive data (Article 11(I)). The general definition of consent in Article 5 (VII) no longer includes a requirement that consent must be express. Article 7 also refers to consent only as

having to be "free and unequivocal," and only Article 11(I) relating to the processing of sensitive personal data requires "express and specific" consent. Article 9 elaborates on the general definition of consent as follows: "The consent referred to in Article 7 shall be free and unequivocal and provided in writing *or through any other means that demonstrates it*." (emphasis added) This suggests that in some circumstances "opt-out" consent and "implied" consent (as well as other forms of demonstrating consent) may be appropriate under this law as long as these forms of consent sufficiently "demonstrate" the individual's intent, which they can if the failure to opt out, for example, follows a clear and effective notice of the option to opt out.

We agree with providing for opt-out consent, implied consent and other forms of demonstrating consent in appropriate contexts, as it reflects a recommendation we had made in our earlier comments to the first draft of this bill. For some of the same reasons that "legitimate interest" is a necessary alternative to consent-based processing in the context of big data analytics and other modern information uses, the definition of "consent" itself must be broader and more flexible than the term "express consent" allows. In some contexts, individuals may clearly indicate their intentions or consent by not acting, such as by not opting out of certain uses of their personal information. Closely related to that is the idea that consent may be implied from the actions (or inactions) of individuals in certain contexts. We believe that the current draft provides for the necessary context-specific flexibility on the appropriate form of consent. However, we also have seen divergent English translations of Article 9, which causes some confusion on the intent of this article. To the extent the Portuguese original text is also subject to diverging interpretations, we recommend that the language be clarified.

Best Practices

We also welcome the incorporation of the concept of privacy risk management by controllers and processors in developing best practices standards in Section II, Article 50(1), by providing that in developing such standards, they "shall take into account the nature, scope and purpose of the data processing and of the data, as well as the probability and severity of risks and damages to the individual." The explicit recognition in the current draft of a risk-based approach to crafting and implementing privacy protections is crucial in enabling the modern information economy and innovation. Any data protection law capable of withstanding the test of time must be sensitive to the fact that different types of data and of processing may present different levels of risk and thus require different compliance responses and levels of mitigations.

By way of further clarification, we would recommend that the final law not only require consideration of risk in the context of "establishing best practices standards," but also in implementing and applying such standards in the day-to-day processing activities of the controllers and processors.

Furthermore, we suggest that you also incorporate explicitly the concept of assessing the benefits of data processing to the data subject, the organization and society in any risk assessment or risk management framework. While this is implicit in the current wording of "tak[ing] into account the nature, scope and purpose of the processing …," we would add the terms "benefits to the individual, the organization and society" to this list of considerations to be weighed against the risks.

Finally, we think it would significantly support the goals of such "best practices" if the law specified incentives for organizations to create and implement such best practices standards. For example, companies that have demonstrated their accountability by participating in such standards could be given greater license in using personal data for a broader range of legitimate and beneficial purposes, subject to the avoidance of harm to the individuals.[3]

Anonymous Data

The importance of anonymization of personal data as a tool to exclude such data from this law to enable a broad range of beneficial data uses, such as big data analytics for purposes of scientific research and product improvement and development, cannot be overstated. The draft law clearly recognizes that fact in that it makes clear that it applies only to the processing of "personal data," which is data about an identified or identifiable person, and not to "anonymized data," which means data that "cannot be identified." (Article 5(IV))

However, the draft also provides that where the anonymization is reversed or reversible "by means of reasonable efforts," such data would be subject to the law. (Article 13). We acknowledge and appreciate that anonymization that could be reversed poses a risk to the data subjects. On the other hand, companies should be encouraged to attempt to anonymize data because it reduces the risk to the data subjects. Yet, subjecting companies to an incredibly difficult-to-predict standard of whether an anonymization technique "may" reasonably be reversible provides little incentive to organizations and has little practical utility. Therefore, we support a two-pronged approach. First, anonymized data should be excluded from being covered by this law where de-anonymization (or re-identification) can be accomplished only through extraordinary (rather than "reasonable") efforts. Second, where anonymized data may be de-anonymized through "reasonable" efforts, we believe it should still be deemed anonymous for purposes of this law **if** the anonymization is coupled with additional procedural, administrative and legal protections against de-anonymization or re-identification. Thus, we recommend that the draft law also incorporate procedural, administrative and legal protections, such as enforceable contractual commitments not to re-identify anonymized data, as well as legal prohibitions not to do so, to ensure that all anonymized data may be recognized as such and excluded under the law.[4]

---

[3] For an elaboration on this concept, please refer to a recent white paper by CIPL on "The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society," available at: https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/World_of_Big_Data_Accountability_and_Digital_Responsibility_Sustainable_Data-Driven_Economy_and_Information_Society.pdf.

[4] For a discussion of this approach, *see, e.g.,* U.S. FTC Report, "Protecting Consumer Privacy in an Era of Rapid Change – Recommendations for Business and Policymakers," 2012, *available at*: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; *see also* "Anonymization and Risk" by Ira Rubinstein and Woodrow Hartzog, *available at:* http://papers.ssrn.com/sol3/abstract_id=2646185.

Moreover, the clause "by means of reasonable efforts" in Article 13 raises the question of what qualifies as a "reasonable" effort to de-anonymize and what is an extraordinary effort. Draft Article 13(2) provides that the competent public body "may rule on standards and techniques used in anonymization processes." We recommend that to the extent the clause "by means of reasonable efforts" is retained, Article 13(2) clarify that the competent body may also provide appropriate parameters for the question of what constitutes reasonable and extraordinary efforts relating to de-anonymization.

We believe that without incorporating procedural, administrative and legal protections into the analysis of whether de-identified data is sufficiently anonymized for purposes of taking the data outside the scope of this law and without providing for the establishment of a workable "reasonableness" standard, it would be nearly impossible in an increasing number of cases to achieve "anonymization" for purpose of excluding personal data from this law.

Further, anonymized data sometimes must be re-identified to provide the benefits derived from the insights gained by analyzing anonymized data to individuals. Thus, the law should provide for reasonable standards for re-identification where appropriate, or allow re-identification for the cases in which the requirements for legitimate interest are met. The need for re-identification in some contexts is another reason to supplement technical anonymization measures with procedural, administrative and legal measures to allow the treatment of de-identified data as "anonymized" for purposes of this law even where it can reasonably be re-identified even without extraordinary efforts.

Definition of Research

Read together, Article 7(IV) and Article 11(II)(c) and §3rd, indicate that "research" as a basis for processing under Article 7 also applies to research by the commercial sector, subject to anonymization when possible. It also implies that such research can be done without consent, since under Article 11 §3rd, research undertaken on sensitive data explicitly excludes commercial research without express consent.

We agree that the term *research* should generally cover research pursued by private sector entities for commercial purposes, but would also extend that ability in the case of sensitive data, especially when it is being managed pursuant to an appropriate and effective anonymization (and re-identification) regime. Private sector scientific research for medical purposes, for example, should not be precluded where racial or ethnic information, or data pertaining to health, sexual life and genetic or biometric information may be directly relevant to the study.

Moreover, anonymization as it currently seems to be conceived in the draft law does not appear to be a solution because in such contexts, re-identification must be a possibility. However, the ability to re-identify information currently seems to preclude the status of "anonymized" data under the draft law. We therefore recommend that the issue of private sector research be reconsidered and clarified.

Jurisdiction

Article 3 of the revised draft essentially provides that the law applies to any processing operation regardless of where the processor is headquartered or where the data is located if (1) the processing occurs in Brazil; or (2) the processing is aimed at providing goods or services to persons located in Brazil or involves processing of data of persons located in Brazil; or (3) the data was collected in Brazil.

We believe that this statement of jurisdiction should be refined to make clear that foreign data controllers are not subject to Brazilian privacy law when they are using Brazilian processors to process non-Brazilian data in Brazil. 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 apply the relevant foreign law that applied to the data at the point of collection. Thus, for example, if a Brazilian processor processes data on behalf of an Japanese controller, it must be able to apply the relevant Japanese legal requirements to such data rather than Brazilian law. Applying Article 3(1) to such data processing in Brazil would significantly undercut and incapacitate any Brazilian processing industry that desires to provide services to global clients.

Further, the current draft language is unclear with respect to the meaning of "persons located in" Brazil. To avoid absurd jurisdiction scenarios relating to visitors and tourists, perhaps the provision could be clarified to refer to permanent residents and citizens of Brazil who are located in Brazil at the time of collection or processing.

In sum, in our view, the privacy law's jurisdiction over controllers should extend only to those controllers established and/or located in Brazil or to controllers that are located outside of Brazil but who are directing their services to Brazilian residents and purposefully collecting personal data of Brazilian residents.

International Transfers

We welcome the inclusion of consent as one basis for legitimizing cross-border data transfers. (Article 33(VII).

However, as we discussed in our comments to the earlier draft of this bill, we believe it is important that any legal regime for cross-border transfers should be able to interact with and mirror the full range of cross-border transfer mechanisms available in other jurisdictions and regions. That way, it is possible for global organizations to devise a globally consistent, efficient and frictionless approach to cross-border transfers of personal data.

It appears that while allowing for European-style global corporate rules (EU Binding Corporate Rules (BCR)), the cross-border transfer mechanisms currently included in the draft law still do not reflect mechanisms like the APEC Cross Border Privacy Rules (CBPR) and the APEC Privacy Recognition for Processors (PRP) that were developed by the Asia-Pacific Economic Cooperation (APEC) forum to enable cross-border data transfers.

The APEC Cross Border Privacy Rules for controllers (CBPR) and the APEC Privacy Recognition for Processors (PRP) are enforceable codes of conduct for intra- and intercompany cross-border data transfers by companies that have been reviewed and certified for participation in the CBPR system by an approved third-party certification organization known as an "Accountability Agent."[5] In that sense, they have broader applicability than the intracompany BCR in Europe.

We believe that it is vitally important that Brazil's privacy law allow for systems similar to the APEC CBPR system to facilitate data flows between Brazil and the Asia Pacific region and its 21 member countries,[6] where the CBPR likely will be the dominant cross-border transfer mechanism. Indeed, APEC is currently considering allowing non-APEC-based companies to obtain CBPR certification, which would open the door for direct Brazilian participation in the system. But even without the current CBPR system's being open directly to non-APEC-based companies, it is nevertheless important that new privacy laws enable cooperation and interoperability between all legitimate data transfer mechanisms. Thus we strongly urge Brazil to fully consider the APEC CBPR system and what it entails and to include APEC CBPR-like mechanisms in your menu of cross-border transfer mechanisms.

Further, we recommend that the law include a process whereby recognized entities other than the "competent public body" can review and approve standard contractual clauses, global corporate rules or cross-border privacy rules similar to the APEC CBPR. Any cross-border transfer scheme that relies on the resources of a government authority for case-by-case approval is likely to come under enormous pressure, given the global nature of the information economy and the likely high demand for such approval. Rather than your relying on government authorities only, we recommend the APEC model of employing formally recognized "Accountability Agents" for such purposes, pursuant to rigorous standards and oversight.

It is also important to highlight that joint liability for parties to an international transfer of personal data (assignor and assignee) is harmful for the chain of participants (see Articles 34(1), 35 and 44). If the assignee is a mere processor (or operator), it is unreasonable to make the assignee liable for the acts of the owner of data, unless it acts out of the scope required by the assignor. An excessive onus for the assignee damages the chain of data processors.

---

[5] The CBPR for controllers track and implement the nine high-level APEC privacy principles. The CBPR were finalized in 2011 and are currently in their initial implementation phase. All 21 APEC member economies endorsed the CBPR and expressed their intent to join the system and to recognize the CBPR in their countries. To join the system, an APEC country must have at least one privacy authority that can enforce the CBPR and one "Accountability Agent" that can certify organizations. The current participants are the United States, Mexico, Japan and Canada, and other APEC countries will soon follow. Three Latin American countries (Chile, Peru and Mexico) are APEC members and eligible to join the CBPR system. In February 2015, APEC endorsed a corollary set of cross-border privacy rules for processors, the APEC Privacy Recognition for Processors (PRP). For more information about the CBPR system, please see www.cbprs.org.

[6] United States; Australia; Brunei Darussalam; Canada; Chile; China; Hong Kong, China; Indonesia; Japan; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; The Philippines; Russia; Singapore; Republic of Korea; Chinese Taipei; Thailand; and Viet Nam.

Competent Public Body/Data Protection Authority

We welcome the inclusion in this draft of Article 53, which outlines the specific duties of a "competent public body." We also understand that the decision not to include the creation, definition and conditions of this competent public body (or a data protection authority) was a political choice based on the budget constraints of the Executive Branch. On the other hand, it is our understanding that the initiative for the creation of a federal authority must come from the Executive Branch and cannot arise from the debate of a bill at the Legislative Branch.

The creation of an independent body is crucial for establishing the best system of protection of personal data. Such entity could have a very small structure with federal reach to ensure the rules and policies are uniform nationally. It would also ensure that the adoption of regulations is led by technically capable officials that act independently.

The multidisciplinary nature of the protection of personal data requires the data protection authority to be independent of the different prisms within government. This ensures they address the subject matter in a balanced way, including the aspects of technology and innovation, local and foreign development, consumer protection, safety and security.

Therefore, we highly recommend that the draft of the bill provide for the creation, scope and powers of a federal, technical and independent data protection authority.

Effectiveness

Finally, we strongly recommend that this law be clarified to have prospective rather than retroactive application.

II. Conclusion

Thank you for considering our further comments and recommendations. If you have any questions, please contact Bojana Bellamy, President, Centre for Information Policy Leadership (bbellamy@hunton.com) or Markus Heyder, VP and Senior Policy Counselor, Centre for Information Policy Leadership (mheyder@hunton.com).