Centre for Information Policy Leadership
Hunton & Williams LLP

Compendium of Excerpts of Ministry Bill Comments for May 16, 2016 Letter to Senator Nunes concerning Senate Bill No. 330:

The following are excerpts from the formal comments of the Centre for Information Policy Leadership (CIPL) on the draft privacy bill of the Ministry of Justice relating both to the initial draft of January 2015 and the revised draft of October 2015. They are relevant to comparable provisions in draft Senate Bill No. 330.

1. 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.

2. 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.[1]

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

[1] 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.

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.

3. 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.

4. International Transfers

CIPL welcomes the draft law's approach to cross-border data transfers to the extent it provides for a spectrum of mechanisms that can be used to legitimize transfers of personal data to countries that do not have similar levels of data protection.

We welcome the incorporation of the widely accepted concepts of "standard contractual clauses" and "global corporate standards" or "global corporate rules" (known in Europe as "Binding Corporate Rules" or "BCR"[2]). These concepts are good starting points for positioning Brazil for data transfers with Europe and other countries that recognize these European cross-border

[2] The EU Binding Corporate Rules (including controller rules and processor rules) are legally enforceable internal rules within a corporate family for the processing of personal data that, upon formal data protection authority approval, are a recognized cross-border transfer mechanism under the current EU Data Protection Directive.

transfer mechanisms. However, standard contractual clauses and binding corporate rules have their limitations – the former can result in undue complexity and the latter are limited to transfers within a corporate group and lack scalability. Therefore, while we encourage Brazil to include these options as legitimate mechanisms for international data transfers, we also encourage Brazil to work with experts experienced in these mechanisms, including CIPL, to improve on these mechanisms, to make them more practical and scalable for widespread use by companies of all sizes.

Moreover, given that modern data flows and economic activity are truly global in nature, it is important to include in the menu of choices additional cross-border transfer mechanisms that mirror those that are available in other jurisdictions and regions and that extend beyond intra-company transfers. Thus, we would encourage inclusion of additional mechanisms such as privacy marks and seals and other organizational codes of conduct that are certified by appropriate third parties or a competent authority.

One such example is the APEC Cross-Border Privacy Rules system developed by the Asia-Pacific Economic Cooperation (APEC) forum. The APEC Cross-Border Privacy Rules for controllers (CBPR) and the APEC Privacy Rules for Processors (PRP) are enforceable codes of conduct for intra- and inter-company 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." Enforcement of the CBPR is provided by participating APEC data protection and privacy authorities that have joined the APEC Cross-Border Privacy Enforcement Arrangement (CPEA).[3]

We emphasize that data transfer mechanisms should allow for transfers not only within a global corporate group that has implemented and approved its global corporate rules, but also between unaffiliated companies.

With respect to the requirement in the current draft that the "competent body" authorize these global corporate standards, we encourage that this requirement be modified to recognize the authorizations of such corporate rules by foreign competent bodies, both with respect to the global corporate standards and any code-of-conduct system or cross-border privacy rules system similar to the APEC CBPR. Requiring organizations to seek approval or authorization for their corporate rules from multiple authorities and multiple jurisdictions would result in significant inefficiencies, would undermine the usability and effectiveness of such cross-border transfer mechanisms and may preclude effective scalability for SMEs. This is evidenced by the European experience with BCR, which has resulted in the possibility to now seek authorization from one "lead" authority in Europe in a process of mutual recognition. It is also why the APEC CBPR

[3] 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 US, 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.

require certification under the CBPR in only the one APEC country in which the company or group of companies is headquartered.

Indeed, an effort is underway between APEC and the EU's Article 29 Working Party to explore ways to streamline the CBPR/BCR certification and approval processes where companies seek "dual certification" under both systems. Thus, CIPL recommends that any Brazilian counterparts to these mechanisms be designed so that they become "interoperable" with other similar cross-border transfer schemes, to ensure that companies that have certified or received approval under a non-Brazilian scheme can be deemed authorized in Brazil to the extent the requirements overlap and *vice versa*.

Furthermore, given the ever-increasing need for cross-border transfers of data, to avoid overwhelming any future Brazilian data protection authority, the draft should include a provision that allows for the use of pre-authorized standard contractual clauses both for transfers to controllers and transfers to processors (similar to those in the EU).

Finally, aside from data transfers that are subject to authorization by the data protection authority in Art. 28 and those that are subject to consent in Art. 29, there should be a provision to allow for transfers of personal data in cases similar to the exceptions to consent in Art. 11 of the draft. Thus, transfers of data to third countries should be allowed under the same exceptions that exist with respect to consent for processing of data within Brazil. This is consistent with other privacy laws that also contain restrictions on cross-border data transfers.