COMMENTS OF THE AMERICAN BAR ASSOCIATION SECTIONS OF ANTITRUST LAW AND INTERNATIONAL LAW ON THE PRELIMINARY DRAFT BILL 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 may not be construed as representing the policy of the American Bar Association.

April 30, 2015

I. Introduction and Summary

The Sections of Antitrust Law and International Law (the "Sections") of the American Bar Association respectfully submit these comments to the Preliminary Draft Bill for the Protection of Personal Data (the "Draft Bill") released by the government of 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 Draft Bill. These comments are intended to further this dialogue, and reflect the Sections' experience in international and cross-border privacy 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 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 Draft Bill in particular. The Sections also commend the government for the general consistency with international data protection law evidenced by the Draft Bill. In these Comments, we 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.

These comments make the following suggestions:

- *Definitions.* We suggest that the Draft Bill clarify the standards by which data will be considered anonymous rather than personally identifiable, thereby providing greater guidance on what data types come within the Draft Bill's core coverage.
- *Written Consent.* We suggest that bases for lawful processing in addition to express written consent be considered, and that implied consent be recognized as adequate in appropriate contexts.

- *Data Security.* We suggest that additional flexibility be considered for the data security provisions of the Draft Bill, drawing upon the many years of experience the United States has with breach notification and security laws.
- *Onward Transfer.* We suggest that some method similar to the EU-US Safe Harbor Agreement be considered for legitimizing cross-border transfers.
- *Big Data.* We suggest that several provisions in the Draft Bill be reconsidered to facilitate "big data" analytics, which can provide important societal benefits.

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.

II. Specific Suggestions

A. Definitions of "Personal Data" in the Draft Bill

The scope of any privacy legislation depends in the first instance on the breadth of information that falls within its coverage. The Draft Bill, in Article 5-I, defines "Personal Data" as any "data related to an identified or identifiable natural person, including identification numbers, location data, or electronic identifiers." On the other hand, the Draft Bill defines "Anonymous Data" that falls outside of its coverage as "data pertaining to a data subject that cannot be identified by the controller for the processing or by any other person, taking into account the means that can be reasonably used to identify said data subject" (Article 5-IV). Finally, the Draft Bill recognizes that personal data can be rendered anonymous by "disassociation," which is defined as "the act of modifying personal data so that they cannot be directly or indirectly associated with an identified or identifiable individual" (Article 5-XIV).

This definitional schema sensibly categorizes data by its likely association with an identifiable person. This approach is reinforced by the definition of "Data subject" in Article 5-VI to mean the "natural person to whom the personal data processed refers," which is consistent and in line with the scope of the legal protection: the personality and dignity of individuals.

However, unlike the laws of other jurisdictions, the Draft Bill does not provide clear guidance as to what level of "disassociation" is sufficient to render otherwise personal data anonymous. Such clarity would allow a data processor to adopt anonymization means with some confidence that they will be sufficient to meet the law's standards. For example, the EU Data Protection Directive 95/46/EC (amended by Regulation no. 1882/2003/EC) addresses this need by referring to the codes of conduct as a "useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible." Such codes of conduct within the context of the EU Data Protection Directive 95/46/EC are akin to "good practices rules" of the Brazilian proposed bill, set forth in Article 48, which also could be used for the same purposes.

For these reasons, we recommend that the Draft Bill be amended to specifically direct the Data Protection Authority to set appropriate standards for anonymization or de-identification of personal data. One method by which this suggestion could be implemented would be supplementing Article 49-A to read: "The competent body shall establish complementary rules and standards for dissociation measures of personal data (by anonymization or by de-

identification), which are deemed in compliance with the general principles of protection of the data subject's data and rights."

B. The "Written Consent" Requirement of the Draft Bill

Generally accepted principles of international data protection law require that processing of personal data be justified by a "legal basis." This "legal basis," most typically, can be established in several ways. Under the EU Data Protection Directive,[1] for example, a legal basis may be established through mechanisms including (a) consent, (b) compliance with a legal obligation, (c) to protect the vital interests of the data subject, (d) in the public interest or in an official capacity, and (e) legitimate interests pursued by the controller (balanced against the privacy risk to individuals from the processing). Under current EU data protection law, "consent" is defined as "any freely given specific and informed indication" by which the data subject "signifies his agreement to personal data relating to him being processed." Under Article 7(a) of the Directive, consent may be explicit or implicit.

The concept of informed consent of data subjects is, of course, a cornerstone of the gathering, processing, and disclosure of personal information under EU privacy law. However, modern data processing requirements in the consumer sector operate on not only consent, but also a "legitimate interest" for processing. Implicit, or opt-out, consent also is commonly used in online services and mobile applications.

The Draft Bill, in contrast to these principles, relies extensively on requiring formal, written consent prior to any processing of information. Article 7, Section I of the Draft Bill requires consent to be "given in writing or any other means that certifies it," and Article 10 requires disclosure of the specific purpose of the processing, the form and duration of the processing, and other factors. Article 11 of the Draft Bill provides only limited exceptions for obtaining explicit written consent, and notably does not include the "legitimate interest" of the data processor.

Although consent is important, and the procedure specified in the Draft Bill can be a useful mechanism for establishing a legal basis for processing, it should not be the *only* method for establishing that legal basis. Requiring explicit written consent for all processing may actually work against the goal of securing informed consent because consumers are likely to experience "consent fatigue" and may simply check "accept" in all instances simply to move through a transaction or a sign-up flow without meaningfully reviewing such options prior to providing consent.

In the United States, the Federal Trade Commission 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 the context of the transaction, or the company's relationship with the consumer, or are required or specifically authorized by law."[2] This concept captures the need to obtain consent where a

[1] Directive 95/46/EC, Section II, Article 7.

[2] *See* U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,* p. 48 (March 2012).

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 fluidity 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 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 consistent reliance on explicit written consent. Thus, opt-out consent may be appropriate when the collection and use of personal data is in line with the user's privacy expectations and online interactions, while affirmative consent would be required where 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 (1) the Draft Bill include the concept of implied consent, and (2) the Draft Bill include the concept of "legitimate interest," along the lines that concept is described in the EU Directive.

C. Inclusion of Data Security Requirements in the Draft Bill

The Sections recognize that maintaining the privacy of personal information depends significantly on the application and maintenance of adequate security of that data. The Sections commend the Draft Bill for directly addressing this, but the Bill appears to apply a standard of care that, in practice, will be difficult, if not impossible, to meet.

Articles 6 and 42 of the Draft Bill requires companies to adopt "*constantly* updated technical and administrative measures" that are proportional to the nature of the information processed and suitable to protect personal data "from unauthorized access and accidental or illegal destruction, loss, modification, disclosure, dissemination, or any form of inappropriate or illegal data processing."[3] The Sections support a provision that would require processors to evaluate, on an ongoing (rather than "continuous") basis, whether existing safeguards implemented by the processors continue to provide appropriate data protections, particularly in light of industry and technological developments. The proposed standard by which measures must be updated "constantly," however, could impose an overly stringent and costly due diligence requirement on processors that does not provide meaningful additional protections to

[3] Art. 42 (emphasis added).

data subjects. Processors would be compelled to continuously deploy new technical and administrative data protection measures to comply with the law's plain language, rather than deploying new or enhanced safeguards based on evaluations of the existing safeguards' effectiveness at reasonable intervals.

As an alternative to a mandate that would require "constantly updated" technical and administrative measures, the Sections recommend a standard that would require processors to assess their technical and administrative measures periodically, and update them as necessary. Specifically:

> "Art. 42 –The data processor shall ***periodically*** *assess its technical and administrative security measures and* implement ~~constantly~~ updated technical and administrative security measures, ***as necessary***, proportionate to the nature of the processed information and able to protect personal data from unauthorized access and accidental or illegal destruction, loss, modification, disclosure, dissemination, or any form of inappropriate or illegal data processing."

Such an approach would provide a practical framework under which processors still would be required to deploy enhanced safeguards in response to new technologies and threats in a manner that would not dilute the protections intended under Article 42 because processors still would have to ensure that the measures are updated frequently enough to protect personal data from "unauthorized access and accidental or illegal destruction, loss, modification, disclosure, dissemination, or any form of inappropriate or illegal data processing."[4] Further, under the current draft, the periodically updated measures would have to be "compatible with the current state of technology, with the nature of the data, and with the specific characteristics of the processing."[5]

Similarly, prompt and adequate reporting of data breaches is an important standard to protect data subjects from harm following the breach. Article 44 of the Preliminary Draft would require controllers to "*immediately* report any security incident which might damage the data subjects" to the relevant competent body.[6] However, the proposed "immediate" notice standard may cause unintended harm to the data subjects impacted by the security incident and may result in over-reporting to the competent bodies. For these reasons, we recommend revising Article 44 by adopting a more flexible standard whereby controllers would be required to report applicable security incidents to the competent bodies "without unreasonable delay."

Under an immediate notice regime, a controller that becomes aware of a security incident inevitably will focus its initial attention and resources on complying with its notice obligations. Given the proposed rigid timing requirement, the controller may feel compelled to conduct an expedited review and initially gather only enough information sufficient to provide notice. Such notice may occur before the controller has obtained an accurate and complete understanding of the root cause and the scope of the incident, which the controller will need before it can contain

---

[4] *Id.*

[5] Art. 42.

[6] Art. 44 (emphasis added).

the incident and adequately secure the affected systems and data. This would be particularly true in instances where a forensic investigator is required to investigate the incident. The result is that personal data may remain vulnerable to further unauthorized access while the controller is focused on providing immediate notice to the competent body.

An immediate notice requirement also may result in excessive reporting to competent bodies. As an example, a controller that provides immediate notice to a competent body based on an expedited review of the security incident subsequently may determine that the incident is not a reportable event because no personal data was in fact compromised. Such over-reporting would place a strain on the resources of competent bodies, and would make it difficult for competent bodies to accurately determine whether prompt notification to data subjects is warranted. Over time, competent bodies would find it increasingly difficult to evaluate root causes of true reportable events and identify security incident trends that may justify closer monitoring or allocation of resources.

As an alternative to an immediate reporting mandate, language that requires controllers to report security incidents "without unreasonable delay" will help to ensure that competent bodies receive prompt notice, while providing controllers with sufficient time to conduct a proper review of the security incident and mitigate any potential threats to the data subjects.[7] Such an approach also will limit instances in which information provided to the competent body is either inaccurate or incomplete, and help to ensure that notice provided to the competent bodies is accurate and meaningful.

Additionally, the notification requirement appears to apply to *any* data breaches, which will result in over-notification and unnecessary expense by both private parties and the government. It is widely recognized that minor breaches that are not likely to cause any harm to consumers should not be reported to regulators or consumers, because over-reporting of meaningless breaches tends to diminish the attention that consumers will give to significant breaches. For this reason, each of the 48 state and territorial breach notification laws in the United States includes a "harm" theshold before notification is required. The OECD suggests a similar concept in noting that processors should "[p]rovide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects."[8] The Sections would suggest that a similar approach be incorporated in the Draft Bill.

D. Cross-Border Data Transfers

Data are, by nature, portable. The regular use of electronic means to gather, process, store, and transfer data necessarily challenges the efficacy of national regulation of data privacy

[7] The vast majority of the U.S. state data security breach notification laws require notification to potentially affected persons "without unreasonable delay" (or similar language such as "the most expedient time possible"). When determining what delay is reasonable, these laws recognize that the timing of providing notification should be consistent with any measures taken by the data controller to determine the scope of the data security breach, prevent further disclosures, and restore the reasonable integrity of the data system.

[8] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data at p. 16 (2013), available at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

because data easily can be transferred outside of the jurisdiction of a data subject's country of residence or citizenship, and there necessarily are limits on the territorial reach and enforceability of the regulating jurisdiction's privacy standards. Any comprehensive privacy law appropriately addresses the applicability of its laws to portable data, and the Sections recognize the common practice of regulating data flows by transfer proscriptions.

The Sections note, however, that sound data management regularly requires that data be shared and transferred across national boundaries. Enterprises frequently harmonize global operations. Commerce increasingly crosses national borders. Business process sourcing can provide efficient means for service providers in developing markets to provide services in markets that were previously dominated by businesses in developed countries. All of these developments, among others, involve cross-border data transfers, which can be accomplished while still preserving privacy protections in a balanced and workable data protection regime.

Article 28 of the Draft Bill addresses that balance. It prohibits the export of personal data to jurisdictions that do not provide privacy protections "equivalent" to that provided in the Draft Bill. Article 28 also delegates to the competent authority the responsibility to assess the adequacy of the recipient jurisdiction's data protection standards. Article 28 also provides enumerated exceptions to that proscription. These exceptions address particularized situations.[9]

Article 29 further provides that, where the recipient nation is deemed not to meet the Draft Bill's data protection standards and no specific exception applies, personal data may be transferred from Brazil to that country only if specific, particularized consent is obtained from the data subject accompanied by a description of the "nature" of the transfer and a warning of its possible risks.

Finally, Article 30 provides that administrative approval of the transfer (one of the exceptions enumerated in Article 28) shall be given if the data processor adopts standard contractual clauses or binding corporate rules that meet as yet undefined regulatory standards.

Similar to the EU Data Protection Directive, and the last version of the proposed EU Data Protection Resolution, the Draft Bill (Article 28) determines that international transfer of personal data is allowed only for countries that provide a level of protection for personal data that is equivalent to the level established in this law. The level of protection of the country shall be assessed by the competent body, and shall take into consideration (Article 28, sole paragraph): (i) the general and sectorial standards established in the country's legislation; (ii) the nature of the data; (iii) compliance with the general principles for personal data protection established in the law; (iv) the adoption of security measures established in the regulations; and (v) other specific factors pertaining to the transfer.

When the country does not provide a level of protection equivalent to that established by the law, the transfer can be authorized by the user by providing a special consent (Article 29) through a specific statement, different from the consent pertaining to other processing operations and with prior and specific information about the international nature of the

[9] Specifically, exceptions are provided for international law enforcement cooperation; the protection of the data subject's health or safety; transfers authorized by the competent authority by regulation; transfers required or permitted by international agreement; or as necessary for the execution of public policy.

operation, including a warning about the risks involved, in accordance with the vulnerability circumstances of the destination country.

The Sections submit that this approach is structurally sound but that it is missing one key component necessary to make it workable in the context of current data uses. The Draft Bill's approach parallels current EU law in dealing with cross-border data transfers, but lacks the operational exception that is provided by the EU-U.S. Safe Harbor framework.[10] This framework provides an appropriate complement to the legitimizing means currently contained in the Draft Bill as it does to the EU cross-border data transfer restrictions.[11] While model clauses and binding corporate rules are appropriate in some circumstances, a broader means by which an enterprise can commit to the regulating nation's data protection standards on an operational (as opposed to a transactional) basis provides both flexibility for the data processor and enforceable legal obligations that protect the data subject's privacy.

For example, the operation of global human resources, consumer marketing, and financial operations require regular access to and use of personal data, and it often would be impractical (if not impossible) to obtain individualized consent on a recurring basis. Further, standard model clauses often are ill-suited for routine data processing. Providing some means for enterprises to commit to the data protection standards of the Draft Bill on an ongoing, comprehensive basis rather than incurring the transactional costs and process inefficiencies of applying them to each individualized data transfer would balance the desired extraterritorial privacy protections with the practical need for enterprises to operate harmonized systems regardless of business location.

The addition of a systemic means for complying with Brazilian standards in global operations would provide balance to the structure set forth in Articles 28-30.

The Draft Bill provides for exceptions when the transfer may be made even to a recipient in a jurisdiction that does not, in the judgment of the competent authority. provide an equivalent level of protection: (i) international legal cooperation; (ii) protection of the data subject´s or third party´s life or physical safety; (iii) competent body authorizes the transfer based on regulations; (iv) commitment arisen from an international cooperation agreement; (v) public policies.

These exceptions are susceptible to the same administrative process inefficiencies faced by enforcers of similar EU regulations, namely the burdensome and lengthy task of waiting for the competent body´s analysis and approval. The Draft Bill is not clear on the how the competent body will function (or even which body will acquire the authority to oversee the application of the data protection law), or how it will verify the same level of protection, issue standard clauses or analyze internal regulations. The Sections respectfully submit that the methodology should be more streamlined and less bureaucratic.

---

[10] For a description of that framework, *see* http://export.gov/safeharbor/.

[11] The Sections recognize that the Safe Harbor framework is the subject of debate within the EU, but believe that it has proven to be a workable and efficient means to maintain EU data protection standards for data processed and accessed in the United States, serving both the privacy of EU data subjects and commercial needs, while preserving comity within the international data protection structure.

E. "Big Data" Issues and the Principles of the Draft Bill

Digital information increases in value when it is combined with other data sets to enable analysis and synthesis, often resulting in additional and new insights. This often is referred to as "Big Data." "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 "Thee Vs").[12] The algorithms seek out probabilistic connections between data elements. There are tremendous potential benefits that can be obtained from the insights of data analytics. Participants at a public workshop hosted by the United States Federal Trade Commission recently addressed the utility of Big Data -- in the areas of medicine (to provide oncology diagnoses and treatments to non-specialists in underserved communities including eligibility for trials) and education (to identify and provide early intervention to "at risk" students).[13] At the same time, the Commission raised concerns about whether data analytics may be used in a non-transparent way to categorize consumers in ways that may affect them unfairly and unlawfully due to implicit bias.[14] The Draft Bill raises some concerns about whether it will preserve the benefits of data analytics while also protecting against its misuse.

Under the proposed legislation, data analytics would constitute "data processing,"[15] and the law would apply to any entity or person performing data analytics in Brazil or using personal data collected in Brazil.[16] The proposed legislation raises two potential issues – (i) the application of the "general principles" in Article 6 in a manner that will achieve the balance identified above, and (ii) the definition of the data subject's right of review in Article 19 in a similar manner.

The general principles articulated in Article 6, reasonably applied, are consistent with the positive use of data analytics.[17] However, some of the other Article 6 principles, if applied over-broadly, could limit the benefits of data analytics. The principle of "suitability, by which processing must be compatible with the purposes sought and with the data subject's legitimate expectations, according to the context of the processing" should be applied flexibly to data analytics, where a key value of the algorithms is the identification of unanticipated, but valid, correlations between data elements.[18] The principle of "transparency, by which the data subjects

---

[12] UK Information Commissioner's Office (ICO) "Big Data and Data Protection," https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf. For further information regarding the "Three V," *see* http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

[13] FTC, "Big Data: A Tool for Inclusion or Exclusion," https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion ("FTC Hearings"), Panel 3 transcript at1-2.

[14] That is, that past biases can impact and reinforce impermissibly biased judgments based on the data being collected and analyzed.

[15] Article 5(II) ("collection … classification, use … assessment").

[16] Article 2.

[17] For example, the principle of "data quality," which focuses on "the accuracy, clarity, and up-to-date nature of the data," is a critical part of data analytics a "fourth V" in data analytics, "veracity."

[18] The principle of "purpose by which the processing must be performed for … explicit purposes that are known to the data subject" also should be applied in a manner that allows for unanticipated correlations.

must be given clear and adequate information about the performance of the processing" also should be applied in a manner that honors the legitimate intellectual property rights of the party conducting the analysis. While some transparency in the correlations identified may be necessary to avoid implicit bias in the data analysis, it should not include compulsory disclosure of the underlying proprietary algorithms.[19] Finally, there is the principle of "nondiscrimination, by which the processing cannot be performed for discriminatory purposes." As noted by a participant at the Federal Trade Commission hearings, data analytics "[b]y definition … is *always* a form of statistical discrimination."[20] The non-discrimination principle must be applied to protect against invidious discrimination but should not otherwise preclude lawful eligibility decision making.

Article 19 provides the data subject with the right to "request a review of decisions that are based on automated processing of personal data and that affect their interests only, including decisions aimed at defining their profile or evaluate aspects of their personality." Article 19 further imposes upon the data controller the obligation to "provide, whenever requested, adequate information about the criteria and procedures used for the automated decision.[21] As noted above, data analytics is used for making "decisions" about individual "profile[s]" based upon statistical analyses. Disclosure of the "criteria" for the decision making may be appropriate if the criteria to be disclosed, and the circumstances under which that obligation will be imposed, are reasonably defined (for example, the cost of disclosure of multiple obvious criteria for more trivial or non-controversial eligibility decisions may be overly burdensome). Moreover, it is unclear what additional disclosures are encompassed within "and procedures." The Sections submit that it should be made clear that this language does not include the direct or indirect disclosure of proprietary algorithms, recognizing the well-documented negative impact of such a requirement on innovation and foreign direct investment.[22]

III. Conclusion

The Sections appreciate the opportunity to comment on the Draft Bill, and commend the government for its open and transparent process. If the Sections can clarify any of the matters discussed herein or answer any questions, please contact us.

---

[19] *See* Jules Polonetsky and Omer Tene, "Big Data for All: Privacy and User Control in the Age of Analytics," 11 Nw. J. Tech. & Intell. Prop. 239, 270 (2013) ("we propose that organizations reveal not only the existence of their databases but also the *criteria* used in their decision making processes, subject to protection of trade secrets and other intellectual property laws"), http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip.

[20] FTC Hearings, *supra* n. 2, Presentation 1, Solon Barocas, Princeton University presentation.

[21] Article 19, §1.

[22] *See, e.g.*, Robert Bird, Daniel R. Cahoy, "The Impact of Compulsory Licensing on Foreign Direct Investment: A Collective Bargaining Approach." 45 American Business Law Journal (Summer 2008), http://www.personal.psu.edu/faculty/d/r/drc13/Index_files/CL_and_FDI.pdf.