



**Comments of the Information Technology Industry Council in Response to the Colombian
Secretariat of Industry and Commerce's Draft Circular on the Protection of Data and
Allowance of International Transfer of Data**

August 1, 2017

Dear Sir or Madam:

The Information Technology Industry Council (ITI), the global voice of the technology sector, appreciates the opportunity to submit the following comments to the public consultation on the updated draft circular on the protection of data and allowance of international transfers of data.

ITI is the premier voice, advocate, and thought leader for the global information and communication technology (ICT) industry. Our member companies include the world's leading innovation companies, with headquarters worldwide and value chains distributed around the globe. ITI brings together leading Internet services and e-commerce companies, wireless and fixed network equipment manufacturers and suppliers, computer hardware and software companies, and consumer technology and electronics companies.

One of the elements of our mission, in every economy in the world, is to position our companies as genuine partners of government. ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. We do this because we firmly believe that the interests of our companies and industry are fundamentally aligned with those of the economies and societies in which we operate. ITI appreciates this opportunity to continue discussions with the Secretariat of Industry and Commerce (SIC) to reinforce Colombia's potential as a thought leader in the region that combines robust protections with forward thinking regulations, while at the same time positioning the country as a hub for innovation and investment. We respectfully submit the following comments to the Government of Colombia.

The previous draft circular on international transfers and transmissions of personal data set the criteria a country must comply with in order to be considered as providing "adequate levels of protection of personal data." The draft provided a whitelist of the countries the SIC considers to be compliant with such criteria, following the European Union's list of "adequate countries" and adding Albania, Costa Rica, Mexico, Peru, and South Korea.

We commend the SIC for its openness and willingness to receive feedback on the earlier draft of the circular, as well as for taking on board our comments about the unique but effective sectoral privacy system that exists in the United States. We believe the SIC's decision to include the United States in the list of adequate countries in the latest draft circular reflects a rigorous and objective appraisal of the robust privacy protections in the United States that go above and beyond the criteria set forth by the SIC.

Indeed, as we expressed in our previous submission to the SIC, the Fair Information Practices principles (FIPPs) are at the core of the U.S. [Privacy Act of 1974](#) (which governs the collection, maintenance, use and dissemination of personal information by federal agencies) and have formed the foundations of the laws of many economies and international organizations. Since that time, varied approaches to privacy legislation have evolved from these principles, with no single approach showing itself to be inherently superior or better at protecting privacy than another. Different approaches can yield different outcomes



for privacy in different places, based on resourcing, implementation, legal culture, and other elements of domestic context. The United States has long maintained specific sectoral laws for privacy regulation relating to [financial services](#), [healthcare](#), [children's data](#), [credit reporting](#) and [government](#) agencies, among others, together with [State laws](#). The U.S. system embraces a risk-based approach to information practices and leverages the subject matter expertise of agencies that regulate specific sectors.

Rather than pursuing a comprehensive domestic privacy law, these sectoral laws are supplemented with rigorous enforcement of privacy matters under the Federal Trade Commission's general consumer protection mandate, relying on [Section V](#) of the FTC Act, which prohibits "unfair and deceptive trade practices" and confers on the FTC the authority to prevent and punish such practices. The long history of FTC enforcement actions serves as a form of jurisprudence. This model reflects an overall U.S. approach that relies on a discrete separation of powers between the federal government and state and local governments, as well as between the various sector-specific agencies each having their own mandates.

We would, however, like to highlight to the SIC that, unfortunately, some of the wording in this revised draft circular on data transfers, when combined with some terms introduced in Decree 1377 of 2013, has the potential to create confusion for companies and regulators enforcing the norm in the future. We believe it is critically important that, in the interest of legal certainty for all the actors involved, this circular explicitly clarify that the "international transmissions" discussed in the Decree 1377, being sub-types of data transfer, also fall under the scope of this circular on international data transfers.

We are concerned that the consequences of this omission have the potential to produce counter-intuitive, inconsistent and arbitrary applications of Colombia's data protection regime in the future – for example, where the applicability of the circular would be limited to international data transfers made by Colombia data controllers to other data controllers abroad, and not to those transfers made between a Colombian controller and foreign processor (a "transmission", under Decree 1377).

We therefore respectfully suggest that the Government of Colombia simply remove any possibility of such an irreconcilable result by clarifying in the circular that any country-of-destination that is whitelisted in the circular applies to both international data transfers and international data transmissions. This small change would significantly strengthen Colombia's data protection regime by offering legal clarity and consistency for all players that are critical to the Colombian market.

Explicitly including the reference to 'transmissions' would preclude any possible doubts and avoid the potential for inconsistent and arbitrary interpretations. Adequacy mechanisms are designed to facilitate transfers between countries that present an equivalent level of respect to privacy and data protection, so establishing limits depending on the nature of the parties involved in the data flows would defeat the overall purpose of the exercise. Especially considering that in this instance, the type of transfers that would be left out are the ones that are more limited in scope, given that the processor must act in accordance to the instructions set by the controller and cannot act independently.

The absence of an explicit clarification risks creating two parallel and inconsistent sets of requirements within Colombia's data protection law and arbitrarily creates legal uncertainty for specific players in the market, particularly cloud service providers. These providers are essential to Colombia's growth and participation in the global economy because they provide low-cost and accessible infrastructure for budding domestic players.

We once more commend the government of Colombia's leadership in updating the adequacy list and for introducing via the circular a third option for organizations looking to transfer data internationally.



Additionally, as [Statutory Law 1581 of 2012](#) in Colombia empowers the administration to develop modern, forward-thinking supplementary regulations on binding corporate rules and on the certification of good practices in data protection, ITI would like to respectfully offer its expertise and the experience of its members to explore the development of such mechanisms in Colombia, should it be of interest in the future. We wholeheartedly support this goal, which implicitly acknowledges that international data transfers and meaningful privacy protection are not mutually exclusive or antagonistic goals – like Colombia, many existing regimes already reflect the need to preserve multiple approaches to cross-border data transfers without weakening privacy safeguards.

There are a range of instruments available beyond the European inspired “adequacy model”- even the European Commission has acknowledged that the adequacy approach alone is insufficient to handle the pressures and challenges of a hyper-connected world, and drafted the GDPR to include various alternative data transfer mechanisms. These instruments can supplement and even stand alone as the foundation of a more robust and less resource-intensive data transfer model. They include model clauses, [binding corporate rules](#) (BCRs), certifications, independent seals, and multilateral frameworks such as the CBPRs (all explained in attached annex). We recommend that privacy regimes officially recognize and develop alternative co-regulatory tools that will reduce the compliance costs of an international patchwork of data protection regulations and would be delighted to work with the Colombian administration to explore mechanisms that can contribute to advancing Colombia’s leadership role in this field.

Finally, we would like to draw the SIC’s attention to a final minor detail in the draft circular, which could benefit from further clarification or tweaking. We recommend the removal of the recital that deems the United States “adequate” due to Safe Harbor (then Privacy Shield), as it might create confusion. Since the SIC has established, upon a thorough review of the U.S. privacy regime against their criteria of adequacy, that the U.S. privacy regime fulfills that criterion, we ask that anything that can be interpreted as an additional condition for adequacy be removed from the circular. Lastly, we also suggest that the SIC clarify that the whitelist created in this circular applies for data transfers and transmissions performed by public sector entities in Colombia in addition to private sector entities.

We thank the Government of Colombia for permitting us the opportunity to participate in this important discussion to promote a robust, accountability based standard for data protection in Colombia.

Sincerely,

A handwritten signature in blue ink, appearing to read "John Miller", is positioned above the printed name.

John Miller
Vice President for Global Policy and Law
Cybersecurity and Privacy

About ITI. *ITI is the global voice of the tech sector. We advocate for public policies that advance innovation, open markets, and enable the transformational economic, societal, and commercial opportunities that our companies are creating. Our members represent the entire spectrum of technology: from internet companies, to hardware and networking equipment manufacturers, to software developers. ITI’s diverse membership and expert staff provide a broad perspective and intelligent insight in confronting the implications and opportunities of policy activities around the world. Visit <http://www.itic.org/> to learn more. Follow us on Twitter for the latest ITI news [@ITI TechTweets](#).*



Annex

Mechanisms for Cross Border Data Transfer

The APEC CBPRs, though currently limited in their uptake, create a framework whose foundational principles are flexible enough to be adopted on a much broader scale. The principle of “accountability,” a key underpinning of the framework, makes the original data collector legally “responsible” for data by making sure the obligations of the data controller follow the data as it crosses borders. The United States, Mexico, Canada, Japan and Korea are already participating or have committed to participate in the CBPRs, while the Philippines, Chinese Taipei and Singapore have all taken steps to participate, and other APEC economies have signaled their interest in joining. The CBPRs offer a scalable system that holds the potential to be less burdensome to economies and companies than other systems (like EU’s BCRs, which under the Directive had been very resource-intensive, tied to administrative rules, and subject to a complex approval process, but [may become less so under the GDPR](#)).

Model clauses or Standard Contractual Clauses (pre-approved, voluntary contractual commitments that are endorsed by national privacy regulators for providing adequate safeguards with respect to the protection of the privacy for international transfers of data from data controllers to data controllers or from data controllers to processors abroad) are a transfer mechanism that can be a similarly straightforward and low-burden way for organizations to comply with their obligations to protect personal data, even when it is being transferred elsewhere.

Third-party certifications, codes of conduct and privacy seals are also examples of co-regulatory tools that place binding and enforceable privacy commitments on participating organizations while providing compliance certainty for regulators, consumers, stakeholders and other industry partners. We stand ready to offer the SIC our industry’s full expertise as they explore the options for such mechanisms and tools for Colombia.