



**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**

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 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 to be 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 discuss with the Secretariat of Industry and Commerce that will reinforce Colombia's potential as a regional model with robust, internationally recognized privacy protections and forward thinking regulations, and at the same time continue to position the country as a hub for innovation and investment in the rapidly expanding digital economy. Therefore, we respectfully submit the following recommendations to the Government of Colombia.

Privacy, security and trust are central to our member companies' businesses, and we take very seriously our obligation to protect the privacy of consumers including their personal information. ITI member companies have global business operations and thus are subject to privacy regimes around the world.

Informed by our global perspective and broad expertise, ITI encourages governments to develop legislative frameworks to protect the privacy of personal information, encourage innovation, promote the growth of trade and allow the free flow of information. Such a framework would support economic growth in Colombia, increase the competitiveness of Colombian companies, including services companies and small and medium-sized enterprises (SMEs), and improve the capacity of Colombia to support and attract further investments in this sector.



In this regard, we appreciate the opportunity to explain how several important concepts contained in the draft circular that could benefit from a more thorough analysis, as well as clarifications, and revisions.

Data Flows

Data is the life-blood of today's global economy. Firms in every economic sector (e.g. agriculture, air travel, travel and tourism, health, education, energy, consumer goods, and financial services) and of every size are exponentially producing more data over time, and therefore rely on data flows for their most basic, daily operations: communication, file management, HR records transfer, remote contracting, electronic payments, supply chain coordination, research and development, data processing, and so much more. In fact, 75% of the benefits of the internet go to these more traditional industries. At the same time, many new Colombian businesses only exist online and are able to reach global markets from one physical location. Interrupting the operation of the underlying enabling technology, the internet, will always have a direct impact on businesses, particularly SMEs.

The internet is designed to function in terms of the network, not physical borders. Every second, data crisscrosses the globe through network exchange points from users to companies and back again. The internet chooses where to route data based on network congestion to and from data centers, where data can be stored, processed, and analyzed without being tied to one specific location. Data localization actually weakens the norms that have allowed the internet, and, by extension, global economic growth, to flourish for decades. Rather than helping their domestic industries or providing better privacy protections or cybersecurity, these measures are often counterproductive. As numerous researchers have concluded, data localization can harm user privacy and security by requiring storage of data in a single centralized location that is more vulnerable to natural disaster and intrusion.

Protecting privacy is an increasingly difficult task in a world where cross-border data transfers happen every moment of the day. This environment leaves national regulators with the daunting task of implementing national laws to protect the privacy of citizens whose data is often located beyond national borders and scattered across various jurisdictions.

An effective approach to deal with these challenges is to adopt regulatory measures that directly and effectively address the risk of harm to individuals. Data localization measures are shortsighted, difficult to implement, and hardly a foolproof way to address modern privacy concerns. Therefore, the data localization requirements on "personal data" contemplated in the data protection circular are concerning to industry, and would negatively impact Colombia's socio-economic growth and development.



Adequacy Model

While Law 1581 of 2012 established that *“Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia”* (“It is understood that a country offers an adequate level of data protection to comply with the standards set by the Superintendency of Industry and Commerce”), we recommend these standards should be aligned with those previously put forth by the Constitutional Court in judgment C-748 of 2011: *“Adequate levels of protection are understood to be satisfied if their legislation includes: principles embracing obligations and rights of parties and data; And with a protection procedure that involves mechanisms and authorities that effect the protection of information.”*

Recognizing that different countries, based on their respective legal frameworks, cultural backgrounds, and particular necessities, may take different pathways to fulfill these criteria, we suggest that the standards established by the SIC are better aligned with the provisions of the Constitutional Court, instead of creating overly specific and restrictive requirements like those proposed in the draft Circular.

For this reason, we suggest the following adjustment to the wording in Section 3.1 for the standards for data transfer:

- "A) Existence of rules applicable to the processing of personal data.
- B) Normative consecration of principles applicable to data processing.
- C) Regulatory consecration of Rights of the Holders.
- D) Normative consecration of duties of those who perform data processing.
- E) Existence of procedures to ensure the protection of information, which may be administrative, judicial, extrajudicial or private.
- F) Existence of authority(s) in charge of protection of personal data or privacy."

Even with changes, we would like to caution that adequacy criteria alone may not provide a sufficient mechanism to ensure personal data is fully protected or is suitable for all international transfers. The mere existence of an authority in charge of protecting data does not guarantee that it is well-resourced or independent enough to do so, and the existence of rules and principles does not offer any guarantee of robust implementation in a specific country.

We therefore recommend offering multiple modern and more effective avenues through which organizations can transfer data, instead of creating a “whitelist” of countries, which may or may not meet strict privacy standards. Allowing businesses more flexibility to comply with privacy requirements fosters greater accountability.

Adequacy Determination

With regard to the preliminary list of countries included in the proposal, we seek further clarification as to how the SIC has determined the adequacy of the listed countries, as well as the



process for adding to or changing the names on this list moving forward. For example, the list omits the United States, when the United States, in fact, meets the criteria of the aforementioned Constitutional Court judgment. We would respectfully request the reconsideration of this adequacy determination for the reasons below.

The United States has a decentralized, yet robust, legal framework for privacy and data protection, including constitutional protections, federal statutes and oversight, as well as state laws. The U.S. Constitution, above all the Fourth Amendment (protecting against government “searches and seizures”), and well-settled U.S. Supreme Court law grounded in the Bill of Rights provide strong baseline protection for privacy and personal information.

Several federal privacy laws regulate the collection, use and disclosure of information on a sectoral basis, including information in the finance and health sectors; information about children; and information related to consumer credit, insurance, housing, employment, and commercial email. Additionally, the Privacy Act of 1974 (one of the first privacy norms to codify the fair information privacy principles) protects against the improper use of personal data by government agencies, the Electronic Communications Privacy Act (ECPA) regulates the interception of electronic communications, and the Computer Fraud and Abuse Act (CFAA) imposes criminal penalties on unauthorized access to information stored on computers.

The Federal Trade Commission (FTC) has broad authority under the FTC Act to address “unfair or deceptive acts or practices in or affecting Commerce,” that violate consumers’ privacy or place consumers’ data at risk. It also enforces laws that protect consumers’ financial and health information, information about children, and information used to make decisions about credit, insurance, employment, and housing. The FTC has used this authority in a variety of privacy and data security contexts to build a robust data protection and privacy enforcement to protect consumers by bringing enforcement actions against companies engaging in unfair practices harmful to consumers regarding the collection, use and disclosure of information, on the online and offline environments.

There are numerous additional privacy protections under U.S. state law providing an expanded scope of privacy protections, including explicit provisions relating to a right of privacy in several state constitutions, and laws to protect individuals’ privacy in various areas, including requiring companies to disclose details of their data sharing with third parties, limiting employer access to employee social network accounts, and security breach notification laws requiring companies to disclose any computer breaches resulting in unauthorized access to consumers’ personal data.

Controller Liability

The draft circular allows for data controllers to independently determine the adequacy of countries not included in the list of adequate countries provided by SIC, which could be a helpful complement to the challenges presented by an adequacy based regime, if it is properly clarified and provided that data controllers are given sufficient safeguards and certainties that responsible



and accountable self-assessments in this regard will be treated fairly, for instance, in the case of a disagreement with the SIC down the line. The allocation of liability in this case should also not deviate from the existing standard for international transfers.

Accountability Models

Accountability, a principle of fair information practices articulated in the OECD Guidelines, 'ensures that the original collector of the personal information remains accountable for compliance with the original privacy framework that applied when and where the data was collected, regardless of the other organizations or countries to which the personal data travels subsequently'. The APEC Privacy Framework promotes this core principle of accountability by enabling organizations (such as companies) to adopt self-binding mechanisms to demonstrate to regulators that certain minimum privacy protections are applied across the organization no matter where the data is processed. An example of such a mechanism are Cross Border Privacy Rules (CBPRs), which help facilitate cross-border data flows by imposing compliance responsibilities on parties who wish to transfer personal data internationally.

The APEC CBPR system relies on the principle of "accountability," requiring participating companies to certify that their privacy policies and practices are consistent with the APEC Privacy Framework, thus demonstrating to participating economies that cross-border data transfers meet certain minimum privacy protections. A fundamental component of the APEC CBPR system is that independent accountability agents assess that companies' policies and practices comply with the minimum APEC CBPR program requirements. The CBPR System provides a scalable, interoperable baseline set of privacy standards. Rather than adopting localization measures aimed at protecting domestic privacy, Colombia should instead pursue interoperable measures such as the APEC CBPRs, which are more attractive multilateral approaches to alleviate those pressures.

A scheme on international transmissions that restricts the flow of "personal data", which could include nearly all data, as proposed by the draft circular, would be overly burdensome on data controllers and processors operating in-country and globally. This would also severely restrict the most necessary forms of data transfers that individuals and business rely on to conduct daily operations. As a result, Colombia's recent economic growth and broader economic development, which have benefitted from the increased use of digital technologies by Colombian businesses and citizens, would slow considerably. Limitations on international cross-border data flows may also impose significant costs on businesses locally and deter others from making direct foreign investments in the country. These costs are ultimately passed on to the consumer, in the form of raised prices in services, reduced competitiveness in the global marketplace, and limited access to the most innovative and impactful goods and services, such as ecommerce, cloud computing, and data analytics.

This framework would also disadvantage Colombia relative to its global peers that do not use data localization requirements to address their economic or public policy objectives. As a



matter of global competitiveness, the government should continue to promote free flow of information and data across borders, while providing for high standards for personal data protection that do not require data storage, processing, or management.

Thank you for your consideration of these comments. ITI remains committed to this initiative, and we look forward to continuing the conversation in order to ensure that Colombia's data privacy protection regime maintains its role as an economic and innovation leader in Latin America.

Kind regards,

A handwritten signature in dark ink, appearing to read "Ashley E. Friedman", is positioned above the typed name.

Ashley E. Friedman
Director, Global Policy