

U.S. Comments on the Colombian Draft Circular on the Protection of Data and Allowance of International Transfer of Data

The United States appreciates the opportunity to provide comments on the draft circular on the Protection of Data and Allowance of International Transfer of Data (Draft Circular)¹ proposed by the Superintendency of Industry and Commerce (SIC). The United States has significant concerns about the content of the Draft Circular and we ask Colombia to reconsider and to suspend any further action thereon until and unless the Draft Circular has been modified to address the concerns expressed by the United States and other interested stakeholders.

Data and the movement of data are at the center of modern 21st century economies.² The free flow of data within countries and between trading partners is important to firms in every sector of the economy, including traditional and new industries, and particularly for small and medium-sized enterprises (SMEs) that rely on the Internet to reach global markets. Companies rely on communication networks to deliver services and coordinate global accounts, run manufacturing and internal operations, promote and develop a global workforce, and manage global supply chains. Access to digital products and services, such as cloud applications, provides companies with cutting-edge services at competitive prices, enabling them to participate in global supply chains and directly access customers in foreign markets. Consequently, a country's ability to grow economically, innovate, and increase its citizens' standard of living is significantly and increasingly correlated with that economy's data linkages to the rest of the world.

Clearly, the data that is foundational to so much of the activity in the modern global economy needs some protections. These protections should apply equally to data interactions regardless of where they occur, as any gaps in protection fundamentally undermine the effectiveness of any data protection regime. In particular, protections should apply equally to data transfers regardless of whether they are domestic or international. Further, any data protection regime must reflect the reality of how businesses do, and must, interact in a modern global economy. That is, any rules must not remove companies' ability to transmit, store, and process data, which is foundational to so much modern economic activity.

In view of the importance of data flows in the global economy, the requirements for "personal data" contemplated in the Draft Circular are very concerning. The Draft Circular imposes a sweeping rule that is likely to be impossible to administer and highly disruptive of cross-border trade. Indeed, it will likely be tantamount to preventing the storage and processing of data in other countries in many situations. While some of the goals suggested in the Draft Circular (*e.g.*, promoting better privacy protections or cybersecurity practices) may be legitimate, the requirements it sets out do not actually further those goals. To the contrary, the requirements could harm user privacy and security by requiring services suppliers to store data from Colombia

¹ Available at

http://www.sic.gov.co/sites/default/files/normatividad/Proyecto_Circular_Adiciona_capitulo_3_al_titulo_5_transferencia_internacional_de_datos.pdf.

² The consulting firm McKinsey & Company estimates that data flows have surpassed goods trade in terms of contributions to global GDP. See www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

in a domestic location that is more vulnerable to natural disasters or intrusions because the service supplier cannot leverage its larger, global cloud storage infrastructure. Further, any disruption in the cross-border flow of data between Colombia and the United States would have a significant and negative impact on trade in goods and services between our countries. Indeed, the unfortunate trend of data localization measures threatens the global nature of the Internet and global economic growth.

We therefore urge Colombia to reconsider the approach reflected in the Draft Circular and to focus instead on how it could ensure that individual companies adequately protect personal information, regardless of where such information is transferred. Colombia could consider as a model the principles in the Asia Pacific Economic Cooperation (APEC) Privacy Framework which provides for an approach that allows for companies to engage in the cross-border transfer of data while remaining accountable to the domestic law of the territory where the data originates.³ Colombia could also consider the relevant recommendations of the OECD, including the Recommendation on Internet Policy Making Principles, which was endorsed by all 34 OECD Member countries and Colombia, and the 2013 Revised Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. The Guidelines direct that an OECD Member country not restrict the cross-border flow of personal data between itself and another country that observes the OECD Guidelines.

To the extent that Colombia ultimately chooses to continue with an approach that involves a determination of the adequacy of other countries' data protection regimes, we are very concerned with the omission of the United States from the list of countries in Section 3.2 of the Draft Circular that are deemed to provide a level of protection of personal data adequate for purposes of allowing the transfer of personal information from Colombia. We understand that the relevant officials in SIC have communicated with our Embassy in Bogota and representatives of the U.S. Federal Trade Commission (FTC). We ask that you review the Draft Circular in light of the concerns set forth herein and take action to ensure that any final decree avoids an unreasonable or discriminatory effect on trade between Colombia and the United States.

Specific Concerns

Section 3.1:

Section 3.1 of the Draft Circular states that it is necessary for Colombia to establish standards pursuant to Law 1581 so that Colombia can determine which countries provide an adequate level of protection for personal data. But there is little discussion or analysis in the Draft Circular of the standards that Colombia proposes to adopt to implement this provision or how countries' compliance with those standards will be assessed. In particular, there is no explanation of the meaning of any of the six standards set out in Article 3.1, and there is no explanation of how Colombia has (or will in the future) analyze whether countries meet the listed standards.

Therefore, the United States requests clarification on how Colombia has analyzed (and proposes to analyze in future) whether countries offer an "adequate level of protection of personal data." Has Colombia developed detailed interpretations of what the six listed elements entail? What

³ Available at http://mdddb.apec.org/Documents/2016/SOM/CSOM/16_csom_012app17.pdf.

efforts did Colombia engage in to assess the factual record for each country to determine that it meets or does not meet the standards? Did Colombia evaluate any countries that it determined did not meet its standards for an adequate level of protection? Has Colombia established procedures for any other countries to initiate a review of its regime for the protection of personal data?

Section 3.2:

The list of countries in Section 3.2 of the Draft Circular does not include the United States. We would like to understand how Colombia came to this conclusion and respectfully request that Colombia give full consideration to including the United States on this list. We particularly invite Colombia to look beyond individual laws alone and consider the interrelated set of practices, enforcement authorities, and voluntary and enforceable undertakings that combine to form the U.S. privacy protection regime.

The United States has a robust legal framework for privacy and data protection, including constitutional protections, federal statutes and oversight, and state laws. These legal instruments include the Federal Trade Commission Act prohibition on unfair or deceptive practices,⁴ and several other federal privacy laws that 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. There are numerous additional privacy protections under U.S. state law that provide an expanded scope of privacy protections, including explicit provisions relating to a right of privacy in several state constitutions.

At the federal level, the Federal Trade Commission (FTC) is the chief agency for privacy policy and enforcement in the United States. The FTC uses law enforcement, policy initiatives, and consumer and business education to protect personal information. The FTC has brought over 500 enforcement actions addressing a wide range of privacy issues, including over 130 spam and spyware cases, more than 40 general privacy lawsuits, and over 60 cases against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk.⁵ The United States would welcome the opportunity to further discuss and explain the U.S. legal framework for privacy and data protection with relevant Colombian officials.

Section 3.3:

We are very concerned about the rule that seems to be set out in Section 3.3(a) of the Draft Circular. To the extent that this provision would be interpreted to require individuals to give specific consent to individual transmissions of data outside Colombia, we have serious concerns that this approach would greatly hamper the provision in Colombia of services that involve the cross-border transfer of data.

As an initial matter, it is unclear what purpose this proposed requirement would serve. The requirement appears to be limited to transfers of personal information outside Colombia (*i.e.*, it

⁴ See Federal Trade Commission Act, 15 U.S.C. §§ 41-58

⁵ See Federal Trade Commission, Privacy & Data Security Update (2016), available at <https://www.ftc.gov/reports/privacy-data-security-update-2016>.

does not cover data transfers within Colombia). However, to the extent that consent is required for certain transfers within Colombia (e.g., for a doctor to have medical records analyzed) there is no reason for such consent to focus on location; if a patient authorizes the analysis, it is unclear why it should matter if the analysis is conducted in either Bogota, Mexico City, or New York. And where consent is not required for a transfer within Colombia, there is no reason for data export, *per se*, to be subject to different requirements.

Further, administration of consent requirements, particularly location-dependent requirements, is problematic, especially if numerous parties are involved in a transaction. Several examples of the extreme difficulty of administering such requirements are discussed below.

First, take the example of a travel services company providing services in Colombia. How would such a company comply with a specific consent requirement when, in providing travel services in Colombia, it relies not only on its own cross-border transfers of data, but also on the transfer of such data by numerous other entities? Under the proposed requirement, would the agent have to obtain the consent of the traveler before providing his or her name to the foreign hotel or airline; or for the hotel to provide personal data to the restaurant or entertainment show that the traveler sought to book? Similarly, if the traveler paid by a credit card, would the credit card company need to obtain consent before it could transfer funds to any of the affected participants in the transaction, which in turn might involve numerous data processing intermediaries interacting with the foreign entity, each of whom would also arguably need to obtain consent? Obtaining specific consent for all these transfers would be extraordinarily burdensome on both the service suppliers and the customer.

Second, take the case of an insurance company that relies on the cross-border transfer of data to provide services in Colombia. If, for example, a life insurance company sought to reinsure its risk using a foreign reinsurer, the reinsurer would generally need to obtain personal information about policyholders in order to evaluate the risk of a set of policies. Obtaining specific consent from each policyholder before transferring the data out of the country would be greatly burdensome and time consuming. Even if the reinsurer could obtain consent from some policyholders, it might have to eliminate other policies from the reinsurance pool. This could change the risk profile of the re-insurance contract, necessitating renegotiation of the entire contract. And again, a specific consent requirement triggered only by the export of data serves no apparent purpose. If the goal is to ensure maintenance of baseline protections between insurer and re-insurer, those same protections could easily be stipulated contractually without needing to involve the individual policyholder.

An even more difficult problem could arise for companies that already have a large number of Colombian customers and that would immediately be in breach of the rules once finalized. For example, many Colombians use foreign-based e-mail and data storage services. It is unclear how an existing cross-border supplier provider of e-mail services could obtain specific consent from its existing subscribers. While the supplier could ask existing customers to affirm consent for data exports, the company cannot compel its customers to take such action. If customers neglect to respond, but continue to use the service, the supplier might be found to have violated the proposed rule. If that email supplier could not obtain consent from certain subscribers, would it have other options to comply with Colombian law, or would it have to terminate supplier accounts?

These are not isolated examples. Similar questions arise in the context of many other sectors that involve commercial entities in possession of personal information pursuant to long-term contracts, such as a company that prints financial statements for a bank, or processes medical billing reports for a hospital. It would be impractical for either company to obtain consent of all individuals affected by the performance of these contracts after the fact. Does Colombia intend to take legal action against companies engaged in existing, ongoing cross-border data transfers to countries that are not listed in Section 3.2? What mechanisms, beyond consent, does Colombia foresee that would allow for the continued provision services relying on a cross-border transfer of data?

In view of the difficulty of administering a specific consent requirement, the United States urges Colombia to reconsider the structure of Section 3.3 of the Draft Circular and the consent requirement set out in Section 3.3(a) in particular.

Conclusion

For the reasons set out above, we request that Colombia reconsider the Draft Circular and suspend any further work until the concerns of the United States and other interested stakeholders have been fully analyzed and addressed. We would appreciate the opportunity to discuss further with the relevant officials in SIC to ensure that the decree avoids any unreasonable or discriminatory effect on trade between Colombia and the United States.