

**Before the  
DEPARTMENT OF COMMERCE  
National Telecommunications and Information Administration**

Request for Comments	)	
	)	
Developing the Administration’s Approach to Consumer Privacy	)	Docket No. 180821780-8780-01
	)	

**COMMENTS OF THE GSM ASSOCIATION**

GSM Association (“GSMA”) respectfully submits comments to the Department of Commerce (“Department”) and the National Telecommunications and Information Administration (“NTIA”) on NTIA’s request for comments (“RFC”) on developing the Administration’s Approach to Consumer Privacy.

**I. Introduction and Summary**

The GSMA recognizes the value of data as a driver of the digital economy. As personal data increasingly catalyzes innovation and growth, it is critical to protect the privacy and security of that data. The GSMA and its members support innovative uses of data, ranging from enabling elements of the IoT ecosystem, such as connected cars,<sup>1</sup> to providing anonymized and aggregated mobility data to meet the UN Sustainable Development Goals through the GSMA Big Data for Social Good initiative.<sup>2</sup> Protecting privacy is an important consideration for the mobile industry as we look to the future. To meet our goals of enabling innovation while also respecting privacy, the GSMA and its members support the risk-based approach advanced by the Trump Administration (“Administration”) in the RFC. We believe that risk-based frameworks to safeguard personal data and encourage responsible digital governance practices will help build consumer trust and confidence.

---

<sup>1</sup> GSMA Internet of Things Programme, “Automotive & Smart Transport,” available at <https://www.gsma.com/iot/automotive/>.

<sup>2</sup> GSMA Big Data for Social Good Initiative, available at: <https://www.gsma.com/betterfuture/bd4sg>.

The GSMA notes that the user-centric privacy outcomes identified in the RFC reflect globally accepted privacy principles.<sup>3</sup> The GSMA also welcomes the Administration’s emphasis on enhancing interoperability of global privacy frameworks. Since globally accepted privacy principles serve as the foundation for interoperability, GSMA is encouraged that many of these principles are discussed in the RFC. Such principles confer numerous benefits on companies, including providing the basis for a flexible, future-proof framework, enabling consistent treatment of data across global operations and facilitating innovation through cohesive and clear data practices, which also help increase scale and reduce cost. As a result, consumers can benefit from wider choice, improved service quality and lower prices of services.

To support the advancement of regulatory interoperability, the GSMA recently commissioned a report entitled “Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation.”<sup>4</sup> The GSMA also recently released a report on the negative effects of data localization entitled “Cross-Border Data Flows: Realising benefits and removing barriers.”<sup>5</sup> We hope that NTIA finds these reports useful to further promote global cross-border data flows.

## **II. Privacy Outcomes**

The RFC recognizes that flexibility, consumer protection and legal clarity are important elements of an outcome-based approach. The GSMA and its members agree that these three areas are critical to both preserving consumer trust and ensuring continued

---

<sup>3</sup> The 2011 GSMA Mobile Privacy Principles are also aligned with globally accepted privacy principles. The overarching objective of the GSMA Mobile Privacy Principles is to foster business practices and standards that deliver meaningful transparency, notice, choice and control for mobile users. See “GSMA Mobile Privacy Principles,” available at: <https://www.gsma.com/publicpolicy/mobile-privacy-principles>.

<sup>4</sup> GSMA, “Regional Privacy Frameworks and Cross-Border Data Flows How ASEAN and APEC can Protect Data and Drive Innovation,” (Sep. 2018) available at: [https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows\\_Full-Report\\_Sept-2018.pdf](https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf).

<sup>5</sup> GSMA, “Cross-Border Data Flows: Realising benefits and removing barriers,” (Sep. 2018) available at: <https://www.gsma.com/publicpolicy/cross-border-data-flows-realising-benefits-and-removing-barriers>.

innovation and growth, in the United States and around the world. While flexibility and legal clarity are often seen as conflicting objectives, a comprehensive future-proof privacy framework based on accountability and the risk-based approach should provide both legal clarity and flexibility for companies to innovate and implement appropriate privacy protections depending on specific business models. Consumer trust is vital to the growth of the digital economy, and privacy protections underpin trust. However, we also recognize that regulatory consistency and fair competition are also crucial to consumer trust and industry growth.

With data being a driving force in the digital economy, it no longer makes sense to treat telecommunications service providers' data differently from data generated by other providers of electronic communications or indeed by the wider digital economy ecosystem. Enacting a national privacy framework that is fit for a digital age necessitates a review of legacy sector-specific rules on privacy to determine whether they are still necessary. In addition, the Federal Trade Commission ("FTC"), as the regulator with the greatest privacy expertise, should generally serve as the enforcement body for the U.S. privacy legislative regime.

From a global perspective, the GSMA notes that in many countries around the world, a misalignment exists between national and/or market-sector privacy laws, such as the misalignment between the European Union ("EU") General Data Protection Regulation ("GDPR") and the EU ePrivacy rules.<sup>6</sup> Such inconsistencies in privacy requirements across different services and applications can result in consumer confusion. Furthermore, some online services and application practices will result in consumers 'consenting' to privacy-

---

<sup>6</sup> This refers to the existing Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ("ePrivacy Directive"), and Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC ("ePrivacy Regulation").

related terms and conditions without reading the notice or understanding the implications of their decisions. The GSMA's commissioned research shows that 82% of users agree to privacy notices without reading them because they tend to be too long or legalistic.<sup>7</sup> Because of the often misunderstood distinction between mobile network operators ("MNOs") and the other services that users access via their mobile devices, there is also the risk of consumers being unaware of who is handling their data.

The GSMA urges NTIA to cooperate with the Federal Trade Commission ("FTC") to ensure a consistent approach and effective overarching user-centric privacy framework that applies consistent rules to functionally equivalent data irrespective of business sector or technology. Future-proof rules require a common approach to all industries. Sector-specific privacy regulations are obsolete in today's dynamic environments and should be withdrawn. It is important to have a level playing field in relation to the regulation of privacy and to ensure functionally equivalent data such as geolocation data is subject to a single set of rules that is neutral regarding technology and business models.

For example, mobile network operators are now subject to additional rules in relation to ensuring the confidentiality and security of consumer proprietary network information ("CPNI"), where other online service providers that capture functionally the same information are not. This imposes additional costs and resource burdens without enhancing the privacy of consumers. Instead, it drives dual standards that do not provide consumers with consistent privacy experiences and protections. The converged and rapidly changing digital ecosystem necessitates a rethink about the level playing field for the use of data by platforms and telecommunications service providers.

---

<sup>7</sup> GSMA, "Mobile Privacy: Consumer research insights and considerations for policymakers" (Feb. 2014), available at: [http://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/GSMA2014\\_Research\\_MobilePrivacyConsumerResearchInsightsForPolicymakers.pdf](http://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/GSMA2014_Research_MobilePrivacyConsumerResearchInsightsForPolicymakers.pdf)

As a result, the GSMA suggests the Department consider the impact of this misalignment on the outcomes advanced by the Administration. For example, in the context of transparency, MNOs are subject to notice requirements under the CPNI rules enforced by the FCC<sup>8</sup>. A divergent approach to transparency and other outcomes creates uncertainty for consumers and MNOs. Additionally, in the context of the Department's efforts' to enhance cross-border data flows, lack of clarity regarding the jurisdiction of the FTC and the FCC makes participation in the APEC CBPR system more difficult. Establishing the FTC's jurisdiction clearly would thus strengthen the APEC system as well.

The mobile industry has made considerable investments to enable safe and secure use of its services, and to also protect the privacy of its customers. The industry, supported by the GSMA, has been highly active in programs to educate consumers and businesses in how to safely use mobile technologies and the applications they support, in order to minimize risks to their data. Minimizing risk requires a holistic response involving various stakeholders, including governments, other mobile ecosystem players, as well as the ultimate providers of services delivered online or via mobile devices.

The dynamic nature of the mobile ecosystem makes this stakeholder collaboration essential. When companies access products and services in a mobile environment, they are often interfacing with different types of companies to enable a seamless experience. Governments and the wider ecosystem should collaborate to ensure that practical solutions enable consumers to make informed and effective choices, balancing each individual's desire for privacy with their desire to access interesting, advertising-funded content and applications from a mobile device.

---

<sup>8</sup> Notice required for use of customer proprietary network information, 47 CFR § 64.2008, available at: <https://www.law.cornell.edu/cfr/text/47/64.2008>.

### **III. Enforcement**

The FTC has decades of experience regulating privacy practices. To avoid duplicative or inconsistent requirements, we believe that a federal privacy framework should be overseen exclusively by the FTC. While some sectoral exceptions may remain, as we noted in the previous section, the privacy of functionally equivalent data should be regulated the same way to ensure a level playing field. In some cases, this would require the FTC to have authority over the privacy practices of service providers currently regulated by the FCC.

### **IV. Global operations and Interoperability**

The evolving global economy depends on the free flow of goods, services, and data, and interoperable global privacy frameworks facilitate and grow this dynamic economy. The privacy outcomes identified in the RFC reflect the globally accepted fair information practice principles (“FIPPs”), which serve as a foundation for privacy laws and frameworks around the world. Privacy frameworks aligned with these principles allow companies to treat data consistently across their operations, innovate more rapidly, achieve larger scale and reduce costs. As a result, consumers can benefit from wider choice, improved service quality and lower prices of services. The Administration’s approach reflects these principles, and adoption of this approach would make it easier for U.S. companies to provide goods and services in other countries, while also benefitting from domestic growth and innovation.

While the United States considers ways to enhance cross-border data flows, other countries around the world have sought to stem the flow of data, for example through requirements to use local servers.<sup>9</sup> In response to the rising incidence of data localization measures around the world, the GSMA issued a recent report, “Cross-Border Data Flows: Realising benefits and removing barriers.”<sup>10</sup> This report includes six recommendations for

---

<sup>9</sup> *Supra* note 4, at page 72 (citing work conducted by the European Centre For International Political Economy (“ECIPE”) on growing data localization measures).

<sup>10</sup> *Supra* note 5.

governments to unlock the benefits of cross-border data flows for individuals, organizations, governments and the economy, while ensuring sufficient data privacy rules are in place to protect citizens and maintain their trust in the digital ecosystem. The recommendations are as follows:

- Recommendation 1: Commit to facilitating cross-border data flows and removing unnecessary localization measures
- Recommendation 2: Ensure privacy frameworks are fit for a digital age
- Recommendation 3: Review legacy sector-specific privacy rules
- Recommendation 4: Encourage regional data privacy initiatives
- Recommendation 5: Avoid localization by addressing foreign surveillance concerns pragmatically
- Recommendation 6: Avoid localization by addressing law enforcement and national security concerns pragmatically

Recommendation 2 encourages governments to base national privacy frameworks on commonly accepted privacy principles.<sup>11</sup> The Administration’s approach aligns with this element of the recommendation. This recommendation also notes that privacy frameworks should operate on a technology and sector-neutral basis so customers are assured of consistent treatment of their data.

To facilitate cross-border data flows, the GSMA is supportive of regional privacy initiatives such as the Asia Pacific Economic Cooperation (“APEC”) Privacy Framework and Cross Border Privacy Rules (“CBPR”). These regional frameworks are based on globally accepted privacy principles, and on ensuring that an organization transferring personal data remains accountable for the subsequent use of the data. However, more needs to be done to make these frameworks easier to use, to encourage other regions to adopt similar frameworks and to make the frameworks interoperable. Interoperability creates greater legal certainty and predictability that allows businesses to build scalable and accountable privacy frameworks.

The GSMA is interested in novel approaches to supporting interoperability of privacy frameworks. For example, the GSMA commissioned the report, “Regional Privacy

---

<sup>11</sup> *Id.* at 22.

Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation,”<sup>12</sup> to consider these privacy frameworks – at both the regional and national levels. The objective of the report is to identify specific steps that can be taken to support the evolution and convergence of privacy frameworks in Asia, and do so in ways that meet the growing challenges facing Association of Southeast Asian Nations (“ASEAN”) and APEC regulators. The report suggests several interesting options exist to more formally integrate and harmonize ASEAN’s Framework and the APEC privacy system, some of which are described below. While the options below are based on research conducted on interoperability between the APEC and ASEAN regions, the concepts articulated could also apply to other regions and countries.

One of the options contemplated in the paper is the development of more functional accountability mechanisms, such as the development of voluntary certification schemes that allow private firms and organizations to implement data protection and privacy rules for cross-border transfers of personal data.<sup>13</sup> For example, certification schemes that meet requirements of both the ASEAN Framework on Personal Data Protection and APEC privacy guidelines (such as the APEC CBPR and Privacy Recognition for Processors (“PRP”) System transfer mechanisms) present interesting opportunities to deepen harmonization between ASEAN and APEC. According to consultations with ASEAN and APEC governments conducted for the development of the GSMA report, any regional cross-border data transfer solution should be based on common principles allowing data to be transferred between the member states of each group based on a form of the “equivalence” test.<sup>14</sup> Some of these common principles can be realised between the ASEAN bloc and APEC, others are better

---

<sup>12</sup> *Supra* note 4.

<sup>13</sup> *Id.* at 24.

<sup>14</sup> *Id.* at 25.



suiting to individual ASEAN member economies and APEC, and some pertain to ways in which ASEAN-based organizations and companies may leverage APEC systems.

To develop formal transfer mechanisms, for example between the ASEAN bloc and the APEC economies, it may also be useful for them to engage in a Memorandum of Understanding (“MoU”) outlining each party’s requirements and responsibilities. Another means to implement a formal transfer mechanism could include something similar to Mutual Recognition Agreements.<sup>15</sup>

In the context of enhancing ASEAN’s alignment with APEC, and to potentially enhance data flows between APEC and other regions, APEC could consider allowing non-APEC members states to participate in APEC accredited systems like CBPR.<sup>16</sup> It appears that a number of countries outside of APEC have expressed an interest in APEC CBPR in the context of bilateral trade discussions.<sup>17</sup> Several consultation responses by governments received during the development of the GSMA’s report indicate governmental interest in and support for having non-members participate in the APEC Privacy Framework and its implementing measures, as long as such a mechanism is contingent on a country’s ability to meet the APEC data protection standard.

Unless there are intense efforts by governments and industry to build momentum, this concept is unlikely to come to fruition in the immediate future. One government surveyed for the GSMA report suggested the current focus is, and should be, on how to get existing members of APEC into the APEC CBPR system first.<sup>18</sup> It should be noted that this option and the option above concerning the integration of ASEAN-APEC countries are not mutually exclusive and could be explored in parallel. Indeed, they could be mutually reinforcing.

---

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> *Id.* at 26.

<sup>18</sup> *Id.* at 26.

GSMA’s report notes that there is also potential for governments, including governments within ASEAN, on behalf of firms and organizations based in their jurisdiction, to petition APEC to extend a BCR-type model to allow the CBPR system to operate outside of APEC within a company-level structure.<sup>19</sup> EU and APEC experts have already developed an informal BCR-CBPR “referential” to serve as useful checklist for organizations applying for authorisation of BCR and/or certification of CBPR.<sup>20</sup> This would alleviate the need to formally extend APEC to non-member economies and instead widen the scope of CBPR at the organizational-level. However, this would require significant changes to the current CBPR system.

In addition to our research on enhancing data flows between the ASEAN and APEC regions, we also recently co-signed a letter with a number of other industry associations to support effective mechanisms for cross-border data flows between the Asia-Pacific and Europe.<sup>21</sup> The letter includes the following “call to action”:

...we call upon the relevant authorities from the European Commission, the European Data Protection Board, and the APEC Data Privacy Subgroup to undertake the following:

1. The European Data Protection Board (“EDPB”) should identify the relevant successor subgroup(s) to continue the prior International Transfers Subgroup’s (“ITS”) work with APEC and re-designate a lead rapporteur, as had been previously established by the Article 29 Working Party.
2. The APEC Data Privacy Subgroup should invite this and all other relevant officials to participate in a re-inaugural Joint Working Team meeting at the APEC First Senior Officials’ Meeting in Chile in early 2019. The parties should commit to an ongoing dialogue in this and other appropriate official forums.
3. The Joint Working Team should establish a work plan that continues and extends the BCR/CBPR referential to include certification pursuant to GDPR Article 42.

---

<sup>19</sup> *Id.* at 26-27.

<sup>20</sup> APEC, “Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents” (2014) available at: [https://www.apec.org/~/\\_media/Files/Groups/ECSG/20140307\\_Referential-BCR-CBPR-reqs.pdf](https://www.apec.org/~/_media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf).

<sup>21</sup> GSMA, Centre for Information Policy Leadership (“CIPL”), U.S. Chamber of Commerce, Asia DPO, Internet Association, Asia Cloud Computing Association, ‘Call to Promote Responsible International Data Flows and Enhance Interoperability Between Asia-Pacific and European Data Protection Frameworks’ (October 25, 2018).

4. The Joint Working Team should encourage robust consultations and input from the private sector on the work plan and developments related to international transfer mechanisms, as industry is best positioned to advise on the potential impacts and practical implementation challenges of specific certification criteria and standards.

5. To allow for the identification of certification commonalities, the EDPB should develop baseline certification requirements for processing operations as part of its European Data Protection Seal under GDPR Article 42, against which the APEC CBPR certification requirements can be mapped.

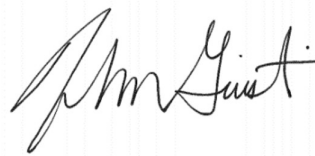
We hope these suggestions prove helpful as NTIA explores ways that U.S. companies can more easily provide goods and services around the world. We look forward to further engagement with NTIA, other governments, and other stakeholders around the world to advance regional and global data flows, and to promote the interoperability of principles-based frameworks.

## V. CONCLUSION

We appreciate the Department's considerations of our views, and welcome further engagement with the Department and the Administration on the development of the Administration's approach to consumer privacy.

Respectfully submitted,

**GSM ASSOCIATION**



By:

John Giusti, Chief Regulatory Officer  
GSM ASSOCIATION  
2nd Floor  
The Walbrook Building  
25 Walbrook  
London, UK  
EC4N 8AF

November 9, 2018