



Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century Project Number P181201

Topic 4 Comments by Twilio

About Twilio

More than two million developers around the world have used Twilio to unlock the magic of communications to improve any human experience. Twilio has democratized communications channels like voice, text, chat, and video by virtualizing the world's telecommunications infrastructure through application programming interfaces (APIs) that are simple enough for any developer to use, yet robust enough to power the world's most demanding applications. By making communications a part of every software developer's toolkit, Twilio is enabling innovators across every industry — from emerging leaders to the world's largest organizations — to reinvent how companies engage with their customers. *Note: The comments below reflect Twilio's initial input on Topic 4. Twilio's full initial comments have been submitted under Topic 1.*

Topic 4: The intersection between privacy, big data, and competition

Twilio recognizes the Commission's emphasis on exploring not just where and by whom data is managed, but on the intersectionality issues of data protection. While the complexity of data and where it's located, how it's processed, and by whom, is increasingly expansive and nuanced, the underlying need to ensure that consumers are protected through privacy and security principles will persist. As a cloud communications provider, Twilio routinely grapples with the interplay between rapidly innovating, new technologies and global efforts at regulations aimed at data protection.

Twilio CEO Jeff Lawson often notes that "Trust is the #1 thing in the cloud." Building and maintaining that trust demands that a cloud-based company act responsibly with regard to personal information entrusted to it, which includes respecting principles of data protection in the handling of that personal information. The promise of the cloud is that the cloud provider can be trusted to fulfill a particular function for its customers better than a customer could do by building it individually because the cloud provider specializes in performing that function and therefore will invest in performing that function well. It follows, therefore, that cloud providers that process personal information as part of their service offerings are expected to perform the function of data protection well, particularly as awareness of privacy concerns grow. In this way, data protection is a competitive advantage. For example, Twilio is ISO 27001 and EU -



U.S. Privacy Shield compliant, invested heavily in the European Union’s General Data Protection Regulation (GDPR) preparedness and had Binding Corporate Rules approved in May 2018.¹

Although Twilio’s preparations for GDPR were resource-intensive and marked by some uncertainty in terms of how requirements applied to Twilio’s unique business model, the process benefited Twilio and its customers by accelerating the maturation of Twilio’s privacy program and adoption of “data protection by design” principles across Twilio’s service and product offerings. As Twilio’s Associate General Counsel Sheila Jambekar CIPP/US, CIPP/E notes: “GDPR is an opportunity to build a stronger data protection foundation which will benefit all.”²

In that spirit, the Commission’s hearings could explore a number of worthy GDPR provisions and evaluate applicability in current and future U.S. rulemaking. In particular, Twilio notes that the GDPR takes a holistic versus sectoral approach, recognizes that different kinds of data require different levels of protection, and distinguishes different roles in how companies act as “Controllers” and “Processors” of data, and how such responsibilities carry different obligations, a concept similar to the HIPAA “covered entity” and “business associate roles”.

For the purposes of the Commission’s upcoming hearings and in consideration of the Commission’s role in enforcing a potential future national regulatory framework, Twilio encourages the Commission to use Topic 4 to examine the costs and benefits of compliance efforts, and with regard to competition, the unique challenges of adhering to multiple legal privacy frameworks for small to medium-sized enterprises.

As companies invest in data protection, uncertainty in existing and future regulation, and the potential for conflicts between different regulatory frameworks domestically and globally introduce operational complexity and inefficiency. For example, Twilio observes lingering uncertainty on implementation and enforcement of GDPR, and potentially conflicting new initiatives such as eEvidence and ePrivacy regulations in the EU, the California Consumer Privacy Act, and the Brazil General Data Protection Law. These operational complexities are often resource-intensive to navigate and may require such things as

¹ See Twilio’s security best practices, including a White Paper: <https://www.twilio.com/security>. In addition to ISO-27001 compliance, Twilio’s multi-factor authentication service offering, Authy, is certified SOC2 compliant.

² See Twilio’s GDPR preparedness, including a White Paper, Data Processing Addendum and information on Binding Corporate Rules: <https://www.twilio.com/gdpr> and Twilio’s White Paper: “Be Prepared for the GDPR: Data protection and privacy”, 2018. Twilio’s White Paper concludes with the observation: “GDPR represents a significant update to the provisions of the Data Protection Directive in an effort to provide appropriate protections for data subjects with respect to how organizations process, transfer, store, and protect the enormous amount of personal data being processed in this new digital world.” https://s3.amazonaws.com/ahoy-assets.twilio.com/Whitepapers/Twilio_Whitepaper_GDPR.pdf



building parallel infrastructure to handle data sets originating from different jurisdictions. As new technology and services are increasingly adopted by users across the country or globally, and not in a single jurisdiction, Twilio urges the Commission to explore how the intersection of multiple regulatory frameworks affects competition.

Offering products or services nationally and globally is no longer just the province of large resource-rich companies. Even small or medium-sized entities can offer products or services to not just a local or national market, but to a global market in today's digital economy. As a result, these operational complexities of handling personal information from various jurisdictions threaten to stymie the global growth of smaller emerging companies and advantage larger organizations that already have sufficient resources to navigate these complexities. In turn, because resource-rich companies can then develop additional products and services based on data sets they have collected, particularly in the machine learning and artificial intelligence (AI) space, only larger companies will have access to the large global data sets needed to build these products for the future.

At the same time, the perception internationally, particularly, in the EU, that the U.S. has lax privacy standards also threatens the competitiveness of U.S.-based companies. In general, Twilio has experienced hesitancy, reluctance, or refusal by European or multinational customers to use its services because they are U.S.-based, despite EU-U.S. Privacy Shield Certification.³ This perception poses a greater threat to smaller or medium-sized cloud-based companies because the only sure solution, today, is to invest in localization of data, which is a significant and resource-intensive undertaking. Accordingly, Twilio proposes that the hearings could further explore how to align any potential future federal U.S. privacy legislation or rulemaking with international frameworks in ways that engender greater confidence in the U.S. data ecosystem and an adequacy determination, without introducing operational complexity.

³ Twilio has certified with the EU-U.S. Privacy Shield Framework and the Swiss – U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of “personal data” (as defined under the Privacy Shield principles) transferred from the European Union and Switzerland to the United States, respectively. <https://www.twilio.com/legal/privacy/shield>