Twilio's Comments on the European Commission's Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts

Introduction

Twilio welcomes the opportunity to engage further with the European Commission on its proposal regarding appropriate rules for the use of Artificial Intelligence (AI). Twilio has already submitted a response to the European Commission's *White Paper on Artificial Intelligence – A European Approach* and to the Inception Impact Assessment on developing requirements for Artificial Intelligence.

Twilio appreciates the risk-based approach the Commission is taking to address AI, and the Commission's efforts to ensure that the huge potential that this technology has is fulfilled. Although still in its early stages, AI is already enabling businesses to deliver high quality engagement with an ever larger number of customers. Today, AI supports businesses in interacting with customers, routing calls and sending emails among many other possible use cases which continue to emerge. However, Twilio is aware that the benefits of this developing technology come with certain risks that need to be managed.

Twilio acknowledges the Commission's efforts in developing a balanced proposal. Further engagement with industry stakeholders as part of developing its legislative approach and ensuring that any legislation is as 'future-proof' as possible is important. While Twilio supports the Commission's overall approach, a number of aspects of the proposal should be reviewed in order to ensure its overall objectives can be achieved.

In particular, Twilio believes modifications in the following areas would ensure that the legislation is more proportionate and effective:

- Clarifying the responsibilities of general purpose software providers
- Defining AI systems appropriately to ensure legal certainty and targeted regulation
- Narrowing the list of AI systems determined to be high-risk
- Turning assessment procedures into guidelines based on standards, not static check-the-box exercises

More details on these points are outlined below, in order of their appearance in the proposal.

About Twilio

Twilio is a leading b2b global cloud operator that enables other businesses, governments and nonprofits to embed communications, such as voice, text messaging, email, chat and video, into their existing web and mobile applications to enhance their engagement with their customers and constituents. Organizations have used Twilio to allow their end-users to contact their teacher or students, alert the public about an emergency, video chat with their doctor, speak with their rideshare driver, make a bank transaction, shop online, authenticate an account, and interact with elected officials, among many other activities.

Twilio provides services to more than 235,000 enterprises globally and powers more than 1 trillion interactions between them and their customers every year. Twilio customers range from small and medium-sized enterprises (SMEs) to the world's largest corporations and come from a broad range of industries including financial services, health care, manufacturing, retail, education, and logistics. They include European and international brands, such as ING and Netflix. Twilio's non-profit arm, Twilio.org, supports charitable organizations to deliver their communications needs, such as the Norwegian Refugee Council, a global NGO supporting refugees worldwide. Twilio is also a technology partner and supporter of the United Nation's Vaccine Alliance GAVI.

Founded in San Francisco in 2008, Twilio now has 26 offices in 16 countries and the infrastructure to support communications worldwide. Trust and privacy have been core principles for Twilio since the company's founding.

How Twilio uses Artificial Intelligence

Twilio leverages AI in order to support the company's mission of enhancing communications. Twilio uses AI and high-quality data training sets to create products that help companies build better relationships with their customers, stop and prevent fraud, and better detect unauthorized log-ins. Our products allow innovative companies to use AI tools that drive efficiency, responsiveness, and customer satisfaction.

Twilio currently offers one AI-powered service, *Twilio Autopilot*. Autopilot is an AI interface that bridges the gap between human agents and self-service bots. It allows developers to build intelligent Interactive Voice Response (IVR) systems, bots, and applications that are powered by Twilio-built Natural Language Understanding and Machine Learning frameworks. Through these technologies, Autopilot is able to turn nested phone trees into simple "what can I help you with" voice prompts and allow customers to use voice search to access a knowledge base. In addition, Twilio is actively looking at ways to incorporate AI into future products that will benefit consumers.

In its internal processes, Twilio works to ensure responsible use of AI, with particular focus on the protection of accuracy, privacy, security and transparency.

Twilio's comments on the Commission's AI proposal

Scope and definition of AI risk capturing non-AI processes

Twilio suggests that the original OECD definition of AI, with an additional clarification (see below), should be used to assess whether an AI system is high risk or not, and that the legislation should be amended accordingly.

The current Commission proposal defines AI systems (Art. 2-3, Annex 1) in a very broad way. Machine learning approaches, logic and knowledge-based approaches and statistical approaches are all included. This creates scope for unintentionally capturing non-AI systems that have either no or a very small impact on an individual's life. For example, the current definition would bring task-routing tools into scope. Among other functions, these tools allow the automatic routing of calls from a UK number to an English-speaking customer service agent. Similarly, airbags in cars have a system that detects if someone is sitting in the front seat, and which will deploy if they sense a crash. No artificial intelligence is involved because the system is unable to learn anything it was not explicitly told by a human to do, and airbag safety is already regulated. Despite this, the current text would mean that systems such as these would fall within the scope of this proposal.

The OECD has established a definition that is much more specific with regard to exactly what constitutes an AI system. It defines one as:

"a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy". (OECD/LEGAL/0449 - Recommendation of the Council on Artificial Intelligence).

Twilio believes that this definition describes those applications that actually constitute effective use of AI more accurately. In order to adequately capture AI applications, it should be slightly amended as follows:

"a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems necessarily operate with some degree of autonomy **in making the prediction, recommendation or decision, though the level of that autonomy may vary from system to system."**

The new legislation already risks limiting innovation and should therefore not go beyond regulating high-risk AI systems. As such, the OECD definition's use within the proposed legislation, refined as proposed above, would create the legal certainty that is necessary for the success of future AI related innovation.

Obligations on AI systems: Software processes differ from products and should not be treated the same way

The conformity assessment procedure should be replaced by a set of guiding principles and standards that are both realistic to implement and flexible enough to grow as AI technology develops further.

The Commission has decided to apply the same approach to the safety of AI systems as to the safety of products (Chapter 2 and Annex IV). However, AI systems consist of a set of software processes which undergo constant development. Products are static at a certain point of their development and when they are certified. As a result, certification exercises based on the AI conformity assessment and leading to a CE certification risk creating a false sense of security.

The proposed conformity assessment takes a static approach to an AI system's status at a certain point in time. Twilio understands that the Commission intends to give existing standardisation bodies a mandate to develop accompanying standards. However, the static criteria used in the current primary legislative text risks limiting the development of AI while failing to make developing AI systems secure.

The key focus of the proposed legislation should be around development of appropriate standards for risk management. For instance, it is unclear which criteria a risk management system must meet to be acceptable, and what happens if a risk was not foreseeable at the time the conformity assessment was conducted, but emerges over time. Requiring error-free and bias-free data does not work because such data does not exist.

The Commission should from the outset work with AI providers to establish appropriate standards. We recommend that the Commission reviews this approach and ensures close cooperation with AI system providers to ensure their requirements are feasible.

Classification of high-risk AI systems needs to be defined more precisely

Twilio believes that the Commission should be more precise in the definition of high-risk AI (Art. 6), and that it should narrow the list of high-risk AI applications (Annex III).

In defining high-risk AI, the guiding principle should be the identification of who is defining the actual intended purpose of the AI system and who determines its parameters. These are the providers who should, in cases of high-risk AI systems, place their products under the scrutiny of further-reaching requirements contained in the legislation.

For instance, if a Twilio business customer builds Twilio's natural language recognition AI tool into an application that supports inquiries about educational and vocational training institutions, the customer becomes the provider who determines the purpose and the parameters, not Twilio.

We note the purpose- and risk-oriented approach used to develop the proposed list of "high risk" AI systems. Under this, the proposal defines high-risk AI systems on the basis of the severity of the potential impact on individuals' lives. However, the list is not sufficiently clear about the exclusion of low-risk functionalities in high-risk environments and may capture AI tools that present no such risk.

For instance, AI systems might be used to determine the time when a critical infrastructure business sends emails to non-paying customers, or an IVR receptionist is used for initial inquiries in an educational institution.

In other cases, the current text might define an AI system as high-risk despite it being composed of low-risk functionalities such as general-purpose software. Such software could, for example, be providing a specific communications support capability for a system that takes further-reaching decisions. Typical applications could be a non-profit hotline catering for social services and natural disaster emergency requests where callers can be quickly routed to the appropriate live agent depending on their needs. While the AI system allows a pre-selection between social service inquiries and other requests, any actual emergency first-response would be done by a human.

General-purpose software in high-risk AI systems must be considered separately

Twilio believes the Commission should clarify explicitly in the legislative proposal's text that the responsibility of compliance with the legislation is considered to be with the provider who controls the purpose. This means the provider of the final AI system is responsible for compliance, not enterprises that are part of the supply chain, and that provide general-purpose software. Twilio understands that this is the Commission's intention, but the legislative text risks causing compliance requirements that general-purpose software providers cannot comply with, for technical and legal reasons.

AI systems often consist of a number of different elements supplied from a number of different providers. Twilio is a b2b provider of AI software. Its customers build Twilio's products into their own b2b or b2c products. The software Twilio provides should be considered as

general-purpose software. It can be built into any kind of use case. Most of these use cases will be low-risk, but Twilio's products can also be used in the context of a high-risk AI use case as defined in Annex III.

For instance, businesses may use Autopilot (Twilio's natural language recognition AI tool) to build and power an IVR bot that delivers advanced response capabilities for interaction with customers. The bot understands dates, names, times and more. While this a low-risk use-case, Twilio Autopilot could also be used for other types of customer interaction that could be considered high-risk in some circumstances, such as emergency hotlines that perform customer routing in order to differentiate between urgency levels. Twilio Autopilot in itself does not have any high-risk intended purpose, but customers might use it to build a high-risk AI system.

The proposal (Art. 24) is not sufficiently clear about where the responsibility for compliance lies in the event that a business customer of an enterprise providing general-purpose software chooses to integrate such a general-purpose software product into a high-risk AI application. General-purpose software providers are unable to perform most elements of the relevant conformity assessment. They are not able to establish and document a post-market monitoring system because the data belongs to, and is managed by, the customer. General-purpose software providers are also not able to foresee the wide array of unintended outcomes. Their business customer determines how the AI system is used and consequently, which unintended outcomes are foreseeable in the context of the chosen purpose.

Twilio suggests that the Commission adopts a similar division of responsibilities as it does in the GDPR, by differentiating between processors and controllers. AI system providers that act as processors should only be responsible for delivering information about the functioning of the AI system and the process for its development. Other aspects of the conformity assessment are in the control of the business customer (and final provider of a potential high-risk AI system) and should be handled by that enterprise.

Governance: need for clarification and differentiation

The Governance framework (Art. 27) is very complex and could involve a wide range of supervisory authorities. This could lead to a situation where certain AI system providers are obliged to report to many such authorities and experience differing outcomes as a result. A harmonized approach is necessary, with a lead authority which is equipped with the necessary expertise and that guarantees legal certainty.

Twilio is concerned about the proposed possibility to access source code of AI. The AI Act currently provides for broad powers for market surveillance authorities to request access, and does not clarify how companies may seek remedies, or how such requests would be issued and justified by the issuing body, and possibly reviewed by the competent judicial authorities. Access to source code should not be within the scope of the relevant authorities.

Conclusion

Twilio believes that AI can be a key driver of business innovation and economic growth in Europe for years to come. A policy framework that encompasses a well calibrated risk-management regime for AI deployment can help foster a trusted AI ecosystem for Europe. Further interaction with AI system providers will be necessary to achieve this. Twilio looks forward to further discussion with the European institutions and to contributing to an AI policy framework that benefits all consumers.