General Considerations on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)

I. Background

The Trans-Atlantic Business Council recognizes the significant work that the European Commission has done on the Digital Single Market initiative to bring EU regulations into the 21st century by encouraging innovation and ensuring adequate privacy protections of European citizens. A central element of a successful strategy is an effective framework on data privacy that works for both consumers and industry.

On January 10, 2017, the European Commission published a proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation) to replace the existing ePrivacy Directive last updated in 2009. The ePrivacy Regulation will apply to any business providing any form of electronic communication services, utilizes online tracking, or engages in direct marketing. The regulation expands the ePrivacy Directive to apply to over-the-top services (OTT) and electronic services where communications is only an ancillary feature.

The new ePrivacy Regulation aims to harmonise the privacy framework related to electronic communications within the EU and ensure consistency with the General Data Protection Regulation (GDPR). The goal is to create new possibilities to process communication data and reinforce trust and security in the EU Digital Single Market.

Unfortunately, the proposal for the ePrivacy Regulation falls short of effectively realizing these goals in two respects.

First, the proposal does not create a technology-neutral framework. Regulation of communication services should be applied in a neutral manner in order to ensure a level playing field for innovation. The GDPR aims to be technology-neutral and sets forth a future-proof framework, while simultaneously guaranteeing a high level of data protection across the different kind of players competing in the data-driven economy. Specifically, Recital 15 of GDPR recognizes that "in order to prevent creating a serious risk of circumvention, the protection of natural persons should be technology neutral and should not depend on the techniques used." The ePrivacy Regulation, as currently drafted, does not achieve this. It subjects providers of electronic communications services to more rigid, burdensome requirements that disproportionately affect possibilities in data analytics in the interest of customers or for public purposes, and discourages development in internet-connected machines that use data.

Second, the proposed ePrivacy Regulation does not achieve the desired alignment with the GDPR. Unlike the GDPR, the ePrivacy Regulation does not recognize the additional legal grounds for processing e-communications metadata which would allow businesses to realize the full advantages of the data-driven digital economy while providing customers real protections and opportunities to control privacy. Such additional grounds are necessary to foster an innovation environment that provides users with new and improved products and services they want and expect.

TABC urges EU decision-makers to assess whether it is necessary to update the ePrivacy Directive given existing legislation and in light of the upcoming GDPR, which already addresses privacy across all sectors of the economy. Given that the proposal is already on the table, it must be fine-tuned to meet its desired

goals and align with the GDPR to ensure that telecommunication and other services are not subject to unjustified additional regulation.

II. A sector-specific approach to privacy regulation in the Internet ecosystem is antiquated and does not meet the privacy needs of the current digital market.

The technology sector has flourished due to expansion of broadband access and consumer demand, leading to a rapid increase in available services and applications. These changes have brought enormous economic benefits to both sides of the Atlantic. They have also reshaped how individuals interact online and communicate via electronic communications. This evolution has real implications to the future of data privacy regulation.

The regulatory framework for electronic communications has not kept pace with the evolution of technology. New services have emerged that, from a consumer perspective, are substitutable to traditional services, but do not have to comply with the same set of rules. It does not benefit industry or consumers for some services to be subject to a conflicting set of data privacy regulations. Consumers expect that their personal data will be protected and kept confidential online, regardless of the application or service used. Regulation should therefore be technology-neutral and horizontal given this convergence trend while relying on sustainable competition.

The United States is coming to terms with the inherent problems with sector-specific requirements to privacy. The Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) are considering strategies to create uniformity by restoring jurisdiction of all Internet services and Internet service providers to a singular regulatory agency – the FTC.

Due to the reclassification of broadband in 2015 as a common carrier, the FCC removed jurisdiction of enforcing data privacy on Internet service providers from the FTC.[1] The FCC's statutory provisions thus applied, and under then-Chairman Tom Wheeler, the FCC adopted broadband privacy rules in 2016. These rules however did not provide the certainty nor the consumer protection that was sought and were ultimately repealed on April 3, 2017.

The rules subjected telecommunication providers to substantially more burdensome provisions than other Internet services that are indistinguishable from a customer perspective. User behavior online and their privacy expectations do not change based on the regulatory classification of the service used. The user provides an Internet service provider with same information as they would to an Internet communications application or social media message application. Further, due to the expansion of web traffic encryption it is unclear whether, as proponent of the rules claim, ISPs are privy to an expansive amount of user information not available to OTT services.

Rather than the erosion of online privacy that was alleged, the repeal set the stage for a comprehensive and uniform approach to consumer privacy. Both FCC Chairman Ajit Pai and Acting FTC Chairwoman support action that would restore jurisdiction to the FTC – leveling the playing field to ensure that all electronic services would be subject to the same rules with respect to user data. As succinctly observed by Ohlhausen, "The federal government shouldn't favor one set of companies over another—and certainly not when it comes to a marketplace as dynamic as the Internet."[2] Chairman Pai recently announced the FCC's

[1] Section 5 of the Federal Trade Commission Act contains a common carrier exemption.

[2] FEDERAL TRADE COMMISSION, Joint Statement of Acting FTC Chairman Maureen Ohlhausen and FCC Chairman Ajit Pai on Protecting Americans' Online Privacy (Mar. 1, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/joint-statement-acting-ftc-chairman-maureen-k-ohlhausen-fcc.

plans to move forward with reforming the 2015 Open Internet rules and remove the Title II classification that would achieve this goal.[3]

Likewise, the EU is taking the lead on updating rules to ensure a comprehensive, level approach to privacy protections in the digital age. The milestone GDPR takes a technology-neutral approach, creating broad definitions that focus on the *use* of the data rather than the characteristics of the entities collecting it. The review of the data protection regime that led to the GDPR was mainly triggered by evolution of technology and therefore adoption of a technology-neutral and future-proof approach. Against that background we would question the need for a sector-specific approach and more importantly, extending its scope by incorporating the definition of "electronic communications services" from the European Electronic Communications Code that extends beyond traditional telecommunication services. Any EU action should further this trend away from a sector-specific approach to data privacy regulation.

III. The ePrivacy Regulation fails to follow the current trend away from sector-specific regulations and creates duplicative and more burdensome regulations for a fraction of the market.

The proposed ePrivacy Regulation does not follow this transatlantic trend. Rather, the proposal subjects electronic communications services to significantly more stringent requirements than other services that process data regardless of the economic value of the data.

The ePrivacy Regulation requires express consent of the end-user for electronic communications services to process communications metadata. To require express consent as the only principal basis for processing metadata would create significant burdens for any third party service that lacks a direct relationship with the consumer, including services like data analytics. It would result in unintended consequences that may diminish the potential benefits to individuals inherent in the technologies and business models by introducing needless delays and interrupting services to obtain new variants of consent.

The consent must also be tied to a specified purpose under the Regulation. However, metadata can be used in a variety of ways not comprehended at the initial collection, or even foreseeable today. The exception as drafted is therefore too narrow and not future-proof. Data controllers and processors recognize the privacy implications when further processing metadata for purposes not known to the customer at the time of collection. That is why we support protections such as those outlined in the GDPR. The GDPR allows the further processing only when there are adequate safeguards in place and sets out a compatibility test.[4] With this compatibility test, with the aid of critical tools such as pseudonymisation, companies can continue to innovate in data analytics while ensuring adequate privacy protections for users.

---

[3] FEDERAL COMMUNICATIONS COMMISSION, Chairman Pai Speech on the Future of Internet Regulation (Apr. 26, 2017), https://www.fcc.gov/document/chairman-pai-speech-future-internet-regulation; The FCC voted favorably to move forward with the Notice of Proposed Rulemaking on May 18, 2017.

[4] The controller, after having met all the requirements for the lawfulness of the original processing has to take into account: (a) Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) The context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) The nature of the personal data, in particular whether special categories of personal data are processes, pursuant to Article 9, or whether personal data related to criminal convictions and offenses are processed, pursuant to Article 10;(d) The possible consequences of the intended further processing for data subjects; (e) The existence of appropriate safeguards, which may include encryption or pseudonymisation. Article 6.4(a-f).

The ePrivacy Regulation also does not recognize "legitimate interests" as a legal basis for processing metadata in line with the GDPR. Under GDPR, the data controller is asked to strike a balance between its legitimate interest and the fundamental rights and freedoms of the data subject which require protection of personal data.[5] The GDPR permits the controller to undertake a thorough assessment, weighing its own interests with the interests and fundamental rights of the user. This approach allows companies flexibility in responding to privacy concerns while still ensuring fundamental rights are protected. It also allows companies to use metadata to deliver routine customer services, including tailored service or for direct marketing purposes.

Conversely, the ePrivacy Regulation is silent on "legitimate interests" and does not allow any flexibility. This lack of alignment severely inhibits routine industry practices. Further complicating compliance, the ePrivacy Regulation fails to include a controller/processor distinction which may be helpful should M2M and IoT continue to be covered.

For these reasons, TABC recommends that the proposed Article 6.1, 6.2, and 6.3 of the ePrivacy Regulations should be modified in order to align with Article 6 of the GDPR by incorporating the additional legal grounds for processing.

IV. The ePrivacy Regulation should not apply to IoT and machine-to-machine communications.

By tying the scope of the ePrivacy Regulation to the proposed European Electronic Communications Code, many new communications services are swept up in the Regulation. The classification of machine-to-machine (M2M) communications as an electronic communication services is inappropriate in this proposal. Recital 12 of the ePrivacy Regulation states that since M2M communications involve "the conveyance of signals over a network", they also constitute an electronic communications service subject to the Regulation. This could mean that various products and services that contain built-in M2M communication features like automated supply chains, remote control or operation of machines might be covered by the legislation. This does not seem to be consistent with the purpose and objective of the ePrivacy Regulation. We see the risk that the inclusion of M2M communications and applying provisions as currently worded would lead to unworkable situations in practice and render standard processes and developments of Industry 4.0 impossible. We suggest a clarification that products and services containing an M2M platform do not fall within the scope of the ePrivacy Regulation.

Today, many companies face the challenge that customers do not only request actions from their machines, but also to related platforms that connect their machines with each other ("M2M platform"). Such M2M platforms essentially consist of the following elements: (i) collection of data from the connected machines, (ii) making the data available to the customer via the platform, (iii) offering functions to analyse the data and (iv) transfer signals to operate and control the machines via the platform. The 'conveyance of signals' may partly be the focus of a service provided via the M2M platform while other services may focus on the delivery of (derived) content. Applying the ePrivacy Regulation to M2M platforms would lead to great uncertainty regarding the legal framework, particularly when the GDPR offers sufficient protection for such types of data processing.

[5] Processing is lawful if necessary for the purpose of the legitimate interests pursued by controller or by a third party, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Article 6.1 (f).

TABC discourages sweeping regulations that will deter further innovation and growth in the Internet of Things – a rapidly changing and not yet mature field. The ePrivacy Regulation should not subject IoT and M2M communications into prospective rules. Any regulations to protect privacy should be flexible enough to adapt as IoT further develops.

The benefits of IoT are not fully realized and to prescribe arbitrary regulations based on outdated notions of consent is ill-advised and not fulfilling of the principles laid out in the GDPR. IoT distinctively creates challenges in obtaining consent from users, often with devices where it is difficult for companies to provide specific notice and consumers to effectively communicate consent. As drafted, the ePrivacy Regulation does not distinguish between personal and non-personal data making explicit consent even more difficult to obtain. The lack of a controller/processor and end-user distinction also do not help on this point.

Existing policy and regulatory approaches on data protection are already applicable to IoT, although concepts of how to apply those rules should be considered in light of the need to expand use of these technologies throughout economic sectors. As in all regulatory constructs, they should be applied in a consistent manner to enhance legal certainty.

V. Conclusion

Strong incentives for continued investment in the EU and the U.S. in secure and high-speed communication infrastructure are necessary to meet the demands of a digital economy and the exponential demands forthcoming in the Internet context in particular. TABC welcomes a privacy framework that will ensure trust in these electronic communications, as the GDPR will do once implemented on May 25, 2018. If the EU decides to implement the new ePrivacy regulation to work in harmony with the GDPR, however, the proposed draft must be altered to ensure the carefully constructed GDPR is realized. It is critical that the supplemental regulation do not alter the careful balance struck in the GDPR to encourage innovation while sensitive to privacy concerns of European Citizens.