THE PENDING EUROPEAN ePRIVACY REGULATION

BY EMILY McCONNELL

What the new legislation means for U.S. companies

THE PHRASE "it's a marathon, not a sprint" is applicable to the world of data privacy regulatory compliance these days. Last year, companies located inside and outside the European Union scrambled to comply with the European Union's far-reaching General Data Protection Regulation (GDPR) – which governs the processing of personal data – before the law became effective on May 25, 2018. The compliance effort is far from over, however. Companies must now devote resources to monitor the development of a new privacy law pending in the European Union: the ePrivacy Regulation (the "ePR"). Many U.S. companies impacted by the extensive compliance requirements under GDPR will be similarly impacted by the equally broad mandates of the proposed ePR.

The purpose of the ePR

When it is finalized, the ePR is expected to replace the current ePrivacy Directive (the "Directive"), which was adopted in 2002 to address the management of subscriber data by telecommunications service providers. In light of the significant evolution in electronic communications over the last 16 years, the Directive is now largely considered obsolete. Accordingly, the ePR aims to modernize current legal rules concerning the privacy and confidentiality of electronic communications. In this regard, the ePR forms part of a comprehensive, ongoing effort by the European Union to reform data protection and privacy laws in the digital age. As such, the ePR is intended to complement and particularize GDPR with respect to any electronic communications data that qualifies as personal data.

The scope of the ePR

Like GDPR, the proposed ePR is very broad in scope. This new regulation would apply not only to traditional telecommunications service providers, but to over-the-top communications services, including instant messaging applications, webmail, personal messaging via social media platforms, voice- and video-calling services, and machine-to-machine, or "M2M," communication services.

The proposed ePR would also protect both the content of electronic communications and the metadata associated with such communications. For example, the timing of an electronic communication, address information of the parties involved in an electronic communication, and geographic location of the terminal equipment of a party involved in an electronic communication would be protected under the current proposal, as well as the actual content contained in the electronic communication.

Moreover, the proposed ePR is not limited to the protection of personal data. It is more broadly concerned with the protection of any and all electronic communications data and metadata – including business data – regardless of whether such information qualifies as personal data.

Finally, the proposed ePR would apply to all instances in which electronic communications services are provided to and used by end users located within the European Union. A company's physical presence within the European Union is irrelevant in determining whether the company is subject to the requirements of the ePR. This effectively translates into worldwide territorial applicability.

The key requirements

The proposed ePR principally addresses the privacy and confidentiality of electronic communications, online tracking and device tracking, and unsolicited electronic marketing communications. Under the proposed ePR, companies would generally be required to collect users' consent to process either the content of, or the metadata associated with, an electronic communication. Such consent would need to adhere to the same consent standard provided in GDPR, which is that it must be:

- Informed and unambiguous,
- Demonstrated by clear, affirmative action,
- Freely given for a specific, agreed-upon purpose, and
- Capable of withdrawal.

In addition, companies would be required to offer users the same electronic communications services regardless of whether such users have provided consent to the processing of their electronic communications data. Online tracking and device tracking would be significantly curtailed under the proposed ePR as well. Operating systems, browsers and other applications would be obligated to require users, upon installation, to choose whether they want to prevent third parties from storing information on their devices or processing information stored on their devices. This centralization of consent in

software settings is intended to eliminate cookie banners and notices on individual websites, which are viewed as ineffective and inefficient. Tracking users through the collection of signals emitted by their devices would be permitted provided that a clear and prominent notice is displayed to the public in the area where such tracking occurs.

Finally, the ePR would require marketers to obtain users' consent prior to sending unsolicited electronic marketing communications, inform users of the marketing nature of the communication and the identity of the marketer, and provide information about how users may withdraw their consent. Direct marketing callers would be required to disclose a contact number or present a specific code or prefix that indicates that the call is a marketing call.

The penalties for noncompliance

The proposed ePR sets forth substantial penalties for noncompliance, which are identical to those set forth in GDPR. Specifically, the proposed ePR provides that violations will be subject to administrative fines of up to 20 million euros or four percent of the violator's total worldwide annual revenue, whichever is greater.

The timeline

The proposed ePR was approved by the European Parliament in the fall of 2017 and was originally intended to come into force on the same day as the GDPR, a date which has now passed. The ePR is currently under review by the Council of the European Union. Before the ePR can be enacted, the Council of the European Union must come to its own consensus on the proposal and then the European Parliament, the Council of the European Union and the European Commission must negotiate the final language in a three-way discussion.

Notably, a spokesman for the then Austrian presidency of the Council of the European Union stated, shortly before the presidency of the Council was turned over to Romania for 2019, "[W]e are not sure if a common position in this topic is reachable. We hope to be able to produce a status report about ePrivacy Regulation."

Thus, it appears highly unlikely that the ePR will come into effect before 2020.

Conclusion

Although the timeline for the enactment of the ePR has decelerated, in light of the proposed breadth of the ePR and the significance of the proposed penalties for noncompliance, companies should take advantage of this extended time frame by dedicating resources to understand what will be expected once the ePR comes into effect and to ensure compliance capability at that time.

Emily McConnell is Corporate Counsel with Equifax and was formerly an attorney in SGR's Corporate Practice in Atlanta.