Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# EU's New E-Privacy Rules Expand Its Authority Over Tech Cos.

By **Allison Grande**

*Law360, New York (January 10, 2017, 10:36 PM EST)* -- The European Commission floated a draft regulation Tuesday that will expose tech companies outside the traditional telecom space — including Facebook, Google and Apple — to stricter privacy rules on electronic communications, but the proposed regime's cross-border uniformity and eased customer-consent requirements could make the changes easier to swallow.

The highly anticipated Regulation on Privacy and Electronic Communications would modernize and replace the bloc's e-privacy directive, which was enacted in 2002 and was last updated in 2009.

While the current directive applies to only traditional telecom providers, the more binding regulation proposed by the European Commission would extend notice, consent, confidentiality and other privacy obligations to cover companies — including "over the top," or OTT service providers — that offer a broad range of electronic communications services such as Facebook Messenger, Gmail, iMessage, Skype, Viber and WhatsApp.

"The new rules are a game changer for all OTT players in the market as they will now be in scope," said Jones Day of counsel Jörg Hladjk, an EU data protection expert who is based in Brussels. "It puts these types of companies in the same box as traditional telcos."

But while these companies will face heightened scrutiny and hefty punishments for noncompliance — the regulation proposes a two-tiered fining system with penalties as high as €20 million or 4 percent of worldwide annual revenue — attorneys noted that the news isn't all bad for electronic communication service providers.

"The general significance is that it brings this part of the privacy regime up to date and in line with the [EU's] General Data Protection Regulation, which hopefully will bring at least more certainty for companies," Ballard Spahr LLP of counsel Odia Kagan said.

European officials approved the sweeping General Data Protection Regulation, or GDPR, last year. The regulation — which is slated to take effect in May 2018 — replaces the bloc's current data protection directive with a uniform regulation that tightens restrictions on the use and flow of data while empowering national privacy regulators to levy fines of up to 4 percent of companies' annual global revenue.

In announcing the new e-privacy regulation Tuesday, the commission confirmed that a main driver behind the update was to make the rules more in sync with the revamped data protection regime, an objective that is likely to make life at least a little easier for large multinationals swept up by both frameworks.

"The draft e-privacy regulation is best understood as an extension of the new General Data Protection Regulation," said Mintz Levin Cohn Ferris Glovsky & Popeo PC member Susan Foster, who is based in London. "The GDPR provides many principles with which companies must comply; the e-privacy regulation gives companies that provide virtually any form of communication services a set of clear rules embodying the GDPR's principles."

Mayer Brown LLP partner Charles-Albert Helleputte, who is based in Brussels, added that while the proposed regulation may "look like a game-changer with many more players being caught by the scope of the e-privacy regulation, one should not forget however that, on the data privacy side, the proposed changes are only a lex specialis to the General Data Privacy Regulation."

However, attorneys were quick to note that while aligning the regimes creates consistency, checking all the boxes for GDPR compliance won't necessarily mean that companies are in step with the e-privacy regulation.

"The e-privacy regulation contains more specific rules for providers of electronic communications services, as their business model is different," Hladjk noted, pointing specifically to the rules surrounding the confidentiality of communications data and how that data is stored.

The e-privacy rules also depart from the GDPR in that they cover communications content and metadata, including the time and location of a call and how long a user spent visiting a website, while the data protection regime targets only personal data.

"Electronic communications content and metadata are a much broader set of information than the personal data covered by the GDPR," Kagan said. "So for those companies that fall under both the GDPR and e-privacy regulation, compliance with GDPR is not going to be enough."

The new regulation covers a wider range of service providers, including companies that may only offer communications as a minor or ancillary feature, such as providing Wi-Fi hot spots in brick-and-mortar stores and user messaging features in apps that don't otherwise allow for communications. Under the regime, those companies will need to take a closer look at the data they collect in order to be ready to comply with their heightened notice and consent requirements, according to attorneys.

"Companies should look at the information they're collecting and make the necessary changes to their consent and notice provisions to reflect that," Kagan said.

But while companies under the new rules will need to do more to inform and get permission from users when they use a broader range of their data, the commission is proposing that at least one provision be relaxed: Once companies obtain this consent to process communications data, they will be free to use it to provide additional services, such as producing heat maps indicating the presence of individuals to help public authorities and transportation companies when developing new infrastructure projects.

The e-privacy rules also clear up a requirement, implemented in 2009, around gaining consent for placing cookies on users' devices, which has resulted in an overload of consent requests for internet users due to widespread confusion and divergent guidance from regulators.

The new rules will allow users to be more in control of their settings by providing them with an easy way to accept or refuse the tracking of cookies and other identifiers. And they'll also clarify that no consent is needed for cookies meant to improve the internet experience but that don't intrude on privacy, such as those that remember shopping cart history and count the number of visitors to a website.

"The virtue of the draft e-privacy regulation is its relative brevity and clarity," Foster noted.

Companies are also likely to benefit from the rules being a regulation that is immediately applicable to all member states upon implementation, rather than a directive that each member state would need to individually transpose into their national laws.

"As with the GDPR, the e-privacy regulation is meant to provide a much greater sense of uniformity and certainty by giving companies one set of rules rather than having to have them abide with 28 different laws," Kagan said.

The draft regulation now goes to the European Parliament and Council, which must sign off on the rules before they take effect. The commission has urged the policymakers to work quickly to put the rules into place by May 25, 2018, which is the date the GDPR is set to enter into force.

"It’s important to remember that this regulation will also be reviewed by the Parliament and Council, so there could be changes," Foster noted. "However, I don’t expect the e-privacy regulation to be significantly softened — the GDPR has already set the stage, and the e-privacy regulation simply has to stay within the GDPR’s strongly privacy-protective principles to get through the legislative hurdles."

--Editing by Mark Lebetkin and Aaron Pelc.

---