SQUIRE PATTON BOGGS

Data Privacy and Cybersecurity
Proposed e-Privacy Regulation Review Moving Forward

There has been considerable activity in the European Union around the proposed e-Privacy Regulation (ePR), which will replace the e-Privacy Directive (aka EU Cookie Directive).

On September 8, 2017, the Presidency of the EU Council (representing the individual EU member states) published proposed amendments to the EU Commission draft. The proposed amendments were circulated in preparation for further meetings with the Working Party for Telecommunications and Information Society (WP TELE) scheduled for September 19, 20 and 25. The compromise text is a working document that will evolve according to the discussions held during the WP TELE meetings. This is only a first redraft, which clarifies certain elements, aligns the ePR text with the General Data Protection Regulation (GDPR) and outlines specific issues to be examined in future EU Council meetings.

Unlike the e-Privacy Directive, the scope of the proposed ePR is much broader in its application to today's electronic communications environment – it includes, among other things, interpersonal communications, machine-to-machine communications and certain over-the-top (OTT) services. In addition, the proposed ePR could significantly affect businesses that are engaged in online behavioral advertising and internet tracking services. Additionally, like the GDPR, the proposed ePR will apply to EU and non-EU companies providing services in the EU. Companies that fail to comply could face fines of up to 4% of a company's global turnover.

The initial compromise text put forward by the Estonian presidency would:

- Simplify the wording of the consent provision and add the obligation that the end-user should be reminded of that possibility consistent with the GDPR (and proposes extending the interval for the reminder to 12 months rather than six months, as proposed by the EU Commission).
- Retain the EU Commission's proposal to allow consent to be expressed via certain technical software settings (and proposes that end-users be asked to consent to the settings upon installation or at the first usage of the software).
- Limit the applicability of the confidentiality provisions relating to machine-to-machine communications to those communications that are "related to the end-user."
- Expand the proposed exemption from the "cookies" provision for audience measurement from first-parties to include "a third party on behalf of the provider of the information society service; provided that the conditions laid down in the (processor contract provision, Art. 28 GDPR) are met".
- Include a new provision allowing for the possibility of class actions for end-users who are natural persons to ensure consistency with the GDPR.

The EU Council presidency's draft sits alongside the amendments being debated in the European Parliament, which has a co-legislator role in the EU process. In June 2017, the EU Parliament published a Draft Report followed by more than 800 proposed amendments (in part 1, part 2 and part 3) to the ePR, tabled by the leading Civil Liberties, Justice and Home Affairs Committee. Similarly, in June 2017, the EU Parliament's Policy Department for Citizen's Rights and Constitutional Affairs published a commissioned study on the proposed ePR. The study concluded that there are four major, high-priority points that should be amended before finalization of the regulation. Of those four points, three relate to the "tracking" of online users, such as through cookies and similar technologies.

- (1) Location Tracking: Article 8(2) should be amended to allow such data collection only with the individual's informed consent, or where such data collection is immediately anonymized (e.g., anonymous people counting).
- (2) Browser and Default Settings: The "Do Not Track" standard should apply to all tracking technologies, including cookies and device fingerprinting – requiring websites to collect affirmative consent from users rather than obtain passive consent via a banner.
- (3) Tracking Walls: The ePR should include specific rules on tracking walls and similar take-it-or-leave-it choices, favoring either fully banning tracking walls or banning tracking walls in certain circumstances (citing to WP29 Opinion regarding five circumstances where tracking walls should be banned).
- (4) Confidentiality of Communications: The analysis of communications content and metadata should only be allowed in limited circumstances and only as is necessary. If no exception applies, companies can analyze their communications content or metadata only after all end-users have given meaningful consent.

Since the EU Commission published its proposed draft of the ePR in January 2017, the Article 29 Working Party (WP29) and the European Data Protection Supervisor (EDPS) have each published comments on the draft. In summary:

- WP29: In April 2017, the WP29 issued an opinion expressing concerns that certain provisions of the proposed ePR are inconsistent with, or set a lower level of privacy protection than, the GDPR. As noted in our prior post, the WP29 is critical of measures relating to Wi-Fi tracking, analysis of content and metadata, tracking walls and privacy by default in relation to terminal equipment and software. The WP29 suggests a number of areas for clarification, such as the scope of the ePR in relation to the persons and member states to which it relates, unsolicited communications, and on the application of consent. The proposed ePR permits the processing of electronic communications data on only a limited number of legal grounds, and the WP29 recommends requiring mandatory consent for analytics, profiling, behavioral advertising, or other commercial purposes.
- EDPS: In April 2017, the EDPS also issued an opinion on the proposed ePR. Among other things, the EDPS considers that the proposed ePR provisions giving end-users the option to prevent tracking applications being placed on their devices does not provide the same standard of protection afforded by Article 25 of the GDPR. The EDPS recommends that hardware and software providers be required to place default privacy settings that safeguard end-users' devices from unauthorized interference. The EDPS also expressed concerns over inconsistencies that may arise between the GDPR and ePR in relation to the protection of personal data.

The EU Commission's proposal anticipates that the ePR will come into effect on May 25, 2018 in line with the GDPR's enforcement deadline. Given the complexity of the issues and the controversy surrounding them, it is generally recognized that the proposed deadline is likely to be extended in future drafts.

Our Data Protection & Cybersecurity team and our EU Public Policy experts are carefully monitoring developments relating to the e-Privacy Regulation and associated legislation, including the EU Electronic Communications Code. Watch this space for further information on legislative developments relating to the ePR.

Contacts

Gretchen A. Ramos
Partner, San Francisco
T +1 415 743 2576
E gretchen.ramos@squirepb.com

Ann J. LaFrance
Partner, San Francisco
T +44 20 7655 1752
E ann.lafrance@squirepb.com

Christina Economides
Public Policy Advisor, Brussels
T +322 627 11 05
E christina.economides@squirepb.com