Digital Single Market – Stronger privacy rules for electronic communications

Brussels, 10 January 2017

Questions and Answers

Why is the Commission modernising EU digital privacy rules?

Since the last revision of the ePrivacy Directive in 2009, electronic communications services have evolved significantly. Consumers and businesses are relying more and more on internet based services to communicate, such as instant messaging, voice over IP and web-based e-mail, but these services are not covered by current ePrivacy rules. By updating the legal framework the proposed Regulation on Privacy and Electronic Communications aims at reinforcing trust and security in the Digital Single Market – a key objective of the Digital Single Market strategy. The draft Regulation also aligns the rules for electronic communications services with the new world-class standards of the EU's General Data Protection Regulation.

Europeans are concerned about their privacy. In a recent Eurobarometer survey, 92% of respondents say it is important or very important that personal information on their computer, smartphone or tablet can only be accessed with their permission, and also 92% state that it is important or very important that the confidentiality of their e-mails and online instant messaging is guaranteed. The proposed Regulation on Privacy and Electronic Communications seeks to address those concerns. At the same time, the new rules will support innovation and increase consumer trust.

What is the Commission proposing?

The cornerstones of the proposed rules on Privacy and Electronic Communications are:

- **All electronic communications must be confidential.** Listening to, tapping, intercepting, scanning and storing of for example, text messages, emails or voice calls will not be allowed without the consent of the user. The proposed Regulation also specifies when processing of communications data is exceptionally permitted and when it needs the consent of the user.
- **Confidentiality of users' online behaviour and devices has to be guaranteed.** Consent is required to access information on a user's device – the so-called terminal equipment. Users also need to agree to websites using cookies or other technologies to access information stored on their computers or to track their online behaviour. The proposal clarifies that no consent is needed for non-privacy intrusive cookies improving internet experience (e.g. cookies needed to remember shopping cart history, for filling in online forms over several pages, or for the login information for the same session). Cookies set by a visited website counting the number of visitors to that website will no longer require consent.
- **Processing of communications content and metadata is conditioned to consent.** Privacy is guaranteed for content of communication as well as metadata – for example who was called, the timing, location and duration of the call, as well as websites visited. Metadata linked to electronic communications have a high privacy component and need to be deleted or made anonymous if users did not give their consent, unless the data is needed for billing purposes.
- **Spam and direct marketing communications require prior consent.** Regardless of the technology used (e.g. automated calling machines, SMS, or email), users must give consent before unsolicited commercial communications is addressed to them. This will in principle also apply to marketing phone calls unless a Member State opts for a solution that gives consumers the right to object to the reception of voice-to-voice marketing calls, e.g. by registering on a do-not-call list. Marketing callers will need to display their phone number or use a special prefix number that indicates a marketing call.

What are the benefits for Europeans and businesses?

- Business and citizens will benefit from **updated rules to reflect technological developments**. The confidentiality of consumers' communications will be protected across the EU, irrespective of

the technology used.

- By replacing the current ePrivacy Directive by a directly applicable Regulation, businesses and citizens will benefit from **one single set of rules across the EU**.
- Cookies and other tracking technologies for online advertisement remain lawful, but will be governed by clearer rules. **Users will enjoy full transparency** without having to click on a banner asking for their consent on cookies each time they visit a website.
- Once users have given their consent, traditional telecommunications services will have **more opportunities to process communication content and/or metadata to provide additional services** and to develop their businesses.
- Users will get **more control over spam and marketing phone calls**.
- The updated rules seek to reinforce **trust and security in the EU's Digital Single Market**.
- **Uniform application of ePrivacy rules across the EU** through enforcement by independent supervisory authorities already competent to enforce the General Data Protection Regulation.

How does today's proposal relate to the General Data Protection Regulation?

The General Data Protection Regulation focuses on data protection for individuals. It was adopted in 2016 and its provisions will apply as from May 2018. The General Data Protection Regulation will enable users to better control their personal data. However, it only applies to the processing of personal data of individuals. It does not cover business-to-business communication or communication between individuals, which does not include personal data. Today's proposed Regulation on Privacy and Electronic Communications complements the General Data Protection Regulation and ensures the fundamental right to the respect of private life with regards to communications.

The new rules also give citizens and companies specific rights and protections, which are not provided by the General Data Protection Regulation. For instance, they guarantee the confidentiality and integrity of users' devices (i.e. laptop, smartphone, tablets), as smart devices should only be accessed if the user has given their permission.

The proposed Regulation also seeks to align privacy rules with the recently adopted General Data Protection Regulation, for example by relying on its definitions. The draft regulation also repeals the security obligations outlined in the current ePrivacy Directive that have become redundant as similar provisions exist in the General Data Protection Regulation.

Will accepting cookies through the browser increase privacy?

The proposed Regulation allows users to make an informed choice when setting up their browser or changing their settings. They will enjoy full transparency and can opt for a higher or lower level of privacy. This is privacy by design, and will end the overload of consent requests for internet users. At the same time, users' internet experience is enhanced as cookies required to ensure the proper functioning of websites will no longer require consent.

Do the new rules mean publishers cannot advertise anymore?

The new rules will not prohibit advertising, or the possibility for websites to use cookies or other technologies for tracking user behaviour. At the same time, the proposal empowers users to make an informed choice concerning the acceptance of these practices. Transparency is important. People must know whether information stored in their devices is being accessed or whether their online behaviour is tracked.

Can users still use ad blockers?

The proposal does not regulate the use of ad blockers. Users have the freedom to install software on their devices that disables the display of advertisement. At the same time, the Commission is aware that 'free' content on the internet is often funded by advertisement revenue. Therefore, the proposal allows website providers to check if the end-user's device is able to receive their content, including advertisement, without obtaining the end-user's consent. If a website provider notes that not all content can be received by the end-user, it is up to the website provider to respond appropriately, for example by asking end-users if they use an ad-blocker and would be willing to switch it off for the respective website.

How will the new rules allow for big data analysis and innovation?

Under the current rules telecom companies can only process traffic and location data for value-added services, such as proposing communications packages better suited to customers' consumptions, or Wi-Fi hotspot in areas of need. They can also process these data for billing purposes so that customers can verify their actual consumption. The new proposal will allow companies to process communication content, and metadata for other purposes if users have given their consent, provided that the company complies with privacy safeguards. This will provide businesses with new opportunities, while at the same time safeguarding Europeans' privacy.

What are the new opportunities for business?

Telecom operators will have more opportunities to process metadata to provide additional services and to develop their businesses. For example, operators could develop heat maps, a graphical representation of data using colours to indicate the presence of individuals. These new services could help public authorities and public transport operators to define where to develop new infrastructures (e.g. roads, metro exits, etc.).

How does the new privacy Regulation deal with encryption?

The proposed Privacy Regulation does not regulate encryption. Ensuring confidentiality requires all providers of electronic communications services to have appropriate security measures in place, as outlined in the Electronic Communications Code and in the General Data Protection Regulation. The latter expressly refers to encryption as an appropriate technical and organisational measure. Furthermore, the proposed ePrivacy Regulation states that providers should inform end-users of the measures they can take to protect their communications and it refers to encryption as an example of such measures.

How is data retention tackled in the proposed privacy rules?

The proposed Privacy Regulation does not harmonise rules on data retention. The proposed Regulation, like the current ePrivacy Directive, contains a provision acknowledging Member States' competence on national security, as enshrined in Article 4(2) of the Treaty on European Union. The draft regulation states that Member States have the right to limit confidentiality of communications of citizens to safeguard one or more of the general public interests referred to in Article 23(1) (a) to (e) of the General Data Protection Regulation. This maintains in particular the existing possibility to limit these rights for reasons related to national security or criminal law enforcement. Member States must govern these restrictions by law; the restriction must respects the essence of the fundamental rights; and they must be necessary, appropriate and proportionate – in line with the jurisprudence of the Court of Justice of the EU (CJEU), including its judgment of 21 December 2016.

Who will enforce the new rules?

The Data Protection Authorities in the Member States, which are already in charge of the rules under the General Data Protection Regulation, will enforce the rules provided in the proposal.

How have companies, public authorities and people been consulted?

The adoption of the Regulation on Privacy and Electronic Communications follows a wide consultation process with industry, national public authorities and civil society. A number of workshops and consultations with stakeholders as well as meetings with expert groups such as the European Data Protection Supervisors and BEREC – the Body of European regulators for Electronic Communications – took place in 2016. A public consultation on the evaluation and review of the current ePrivacy Directive took place from April to July 2016, and a Eurobarometer survey focused on collecting citizens' views on ePrivacy was conducted in July 2016.

What are the next steps?

Today's presentation officially starts the legislative process for the two proposed Regulations. The Commission calls upon the European Parliament and the Council to work swiftly and to ensure their smooth adoption by 25 May 2018, when the General Data Protection Regulation will enter into application. The intention is to provide citizens and businesses with a fully-fledged and complete legal framework for privacy and data protection in Europe by this date.