European Commission

#ePrivacyEU

Towards a future proof legal framework for online privacy

Millions of Europeans make phone calls, send text messages or rely on the Internet to keep in touch with friends and family, share their thoughts, photos and experience or to access essential services like energy or healthcare. Each time a person goes online, to get travel directions, to book a hotel or communicate via instant messaging, they entrust personal information to Internet service providers, telecoms operators or visited websites.

Over the years EU legislation and investments in research and innovation have contributed to an environment where Europeans enjoy the benefits of the digital world in full confidence while fundamental rights to a private and family life, including communications, and the protection of personal data are safeguarded.

EU-wide rules mean that personal data can only be processed lawfully under strict conditions and for a legitimate purpose. These rules are set out in the Data Protection Directive (1995) and in the ePrivacy Directive (1997, updated in 2002 and 2009) – which regulates the processing of personal data and the protection of privacy in the electronic communications sector.

These rules are now undergoing a reform to build a modernised legal framework which will increase trust in the online world and create the conditions for the European Digital Single Market to flourish.

At the end of 2015, the European Parliament and Council agreed on the new General Data Protection Regulation to ensure that Europeans enjoy a high standard of protection for their personal data everywhere in the EU.

This revision process also affects the ePrivacy Directive, which specifically address privacy and data protection in the electronic communications sector. The Commission has launched a public consultation to seek views on the existing legislation, and the possible changes to it. The feedback from the consultation will help the Commission prepare a new legislative proposal on ePrivacy, which is expected by the end of 2016.

What is the relation between the General Data Protection Regulation and the ePrivacy Directive?

The EU's Data Protection and ePrivacy laws are both rooted in the EU Charter of Fundamental Rights, in particular in Articles 8 and 7 which recognise people's right to personal data protection and the respect of private and family life. While Data Protection legislation covers a broad scope and is the reference point for all privacy matters, the ePrivacy Directive mainly focuses on the electronic communications sector, covering services provided by means of electronic signals over, for example, telecommunications or broadcasting networks.

The new General Data Protection Regulation (GDPR)

Since 1995, the EU has put in place rules on data protection to guarantee this citizens' fundamental right. The Data Protection Directive has proven to be a safe anchor point to protect privacy for long time.

However, the lack of harmonisation in the way Members States implemented its provisions created complexity, legal uncertainty and administrative costs, with a negative impact on people's trust and on competitiveness of the EU economy.

Also, back in 1995 there was no privacy issue due to digital services that are extensively used today, such as social networks, cloud computing or smart card, because these services simply did not exist yet.

As a result of a major reform effort, in December 2015 the European Parliament and Council agreed at political level on the new General Data Protection Regulation (GDPR). The GDPR will constitute the single pan-European law on data protection that will deliver a robust set of rules aiming at:

- reinforcing individuals' rights
- strengthening the EU internal market
- ensuring stronger enforcement of the rules
- streamlining international transfers of personal data and
- setting global data protection standards.

Following the political agreement, the final text will be formally adopted by the European Parliament and Council in the course of 2016. The new rules will become applicable two years thereafter.

The ePrivacy Directive

The ePrivacy Directive is part of the EU's regulatory framework for electronic communications, providing a comprehensive set of rules to encourage competition, improve the functioning of telecoms market and guarantee basic user rights.

This Directive complements the Data Protection legislation, by establishing specific rules on privacy for the electronic communication sector. All matters concerning the protection of personal data in the electronic communication sector which are not specifically addressed by the ePrivacy Directive are covered by the EU's broader current and future Data Protection rule.

The cornerstones of the **current rules** on ePrivacy are:

- **confidentiality of communications**: EU Member States must ensure the confidentiality of communications over public networks, in particular by prohibiting the listening into, tapping and storage of communications without the consent of the users concerned.
- **security of networks and services**: a provider of a public electronic communications service has to take appropriate measures to safeguard the security of its services.
- **personal data breach notifications**: providers of publicly available electronic communications services are obliged to notify, according to specific formats and procedures established at EU level, the competent national authorities of personal data breaches. Under specific circumstances users need to be notified, too.
- **confidentiality of terminal equipment**: prior informed consent is required for anyone who wishes to access information from users' mobile phones and computers (e.g. emails, pictures, contacts, etc). It also applies to websites using cookies or similar technology to access information stored on a user's terminal equipment.
- **traffic and location data**: unless the subscriber has given consent to the use of such data for different purpose than communication or billing, they have to be deleted or anonymised.
- **spam and direct marketing**: subscribers must give their prior consent before unsolicited commercial communications ("spam") by automated calling machines, fax or electronic mail are addressed to them. This also covers SMS text messages and other electronic messages received on any fixed or mobile terminal.
- **public directories**: subscribers' prior consent is required in order for their telephone numbers, e-mail addresses and postal addresses to appear in public directories.
- **calling-line identification:** subscribers must be given the option not to have their telephone number disclosed when they make a call.

What does the Commission want to achieve in the field of ePrivacy?

1. Strengthening trust in online world by increasing the security and confidentiality of communications

Under EU law, Member States have to ensure the confidentiality of communications over public networks. The protection of confidentiality communications is enshrined in Article 7 of the EU Charter of Fundamental Rights, together with the respect of private and family life.

Under Article 5(3) of the Directive, storing information, or accessing information already stored in user's device requires his or her permission. The effectiveness of this provision will be evaluated in view of new tracking techniques - such as device fingerprinting – and the need to reassess the list of exceptions to the consent rule.

Increasing the confidentiality of communications will help make Europe more trusted online. Many Europeans use internet-based voice and messaging services instead of, or in addition, to their mobile phones or fixed connections, which is why it is important to guarantee the same level of protection online as offline irrespective of the technology used. The Commission is considering whether the current ePrivacy rules on confidentiality and security need to be extended to cover providers of internet-based voice and messaging services (also known as "over-the-top" services).

2. Boosting the Digital Single Market

For the European single market to function effectively, the huge amount of data that flows across electronic networks and between our phones, smartphones, tablets, computers and other devices needs to freely move within the EU. This objective underpins the existing regulatory framework, and will remain a guiding principle in the review of the ePrivacy Directive. The current EU law foresees the harmonisation of legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data and privacy and provides for the possibility to set up specific rules on technical features and standardisation for terminal equipment.

The Commission also wants ePrivacy to contribute to a thriving Digital Single Market through common rules across the Member States for the relevant market players.

3. Delivering legislation fit for the digital age

In the past few years, important changes have transformed the electronic communication arena, both on the technology side, for example the spread of Internet-based communications services, and in terms of legislation, for example the recent political agreements on the General Data Protection Regulation, the Data Protection Directive for the police and criminal justice sector and the Network and Information Security Directive.

The Commission is now reviewing the existing set of rules in order to build an ePrivacy legal framework that is up to date with the challenges of the digital age and the new legal context.

The review of the ePrivacy Directive: looking backwards to ensure forward-looking ePrivacy legislation

To respond to the new technological and legislative reality, in the Digital Single Market Strategy, the Commission has planned a review of the ePrivacy Directive which is also an element of the overall modernisation process of the data protection framework, with the ultimate aim to strengthen trust in online services.

The Commission is firstly evaluating how the existing rules have performed. In particular, a REFIT evaluation will assess the current provisions of the ePrivacy rules against criteria such as effectiveness, efficiency, relevance, coherence (internally and with other existing regulations) and EU added value.

Without prejudice to the outcome of this retrospective evaluation, the Commission has already identified several policy issues to be potentially tackled with the review. These include:

- ensuring **consistency** of ePrivacy rules with the General Data protection regulation;
- **updating the scope** in light of the new market and technological reality, for example assessing whether to include over-the-top providers (OTT) that offer communication services over the internet (e.g. Voice over IP, instant messaging);
- **enhancing security and confidentiality** of communications;
- addressing issued linked to the **inconsistent enforcement and fragmentation** at national level, such as the co-existence of multiple authorities and its impact in enforcement and harmonisation.

Both the past performance and the possible future options for the ePrivacy rules are part of the public consultation, whose results will feed the preparation of the new legislative proposal.

Research and Innovation in the area of ePrivacy

The pervasiveness of the theme of privacy in ICT has led the European Commission to invest in research and innovation solutions that would help increasing users' privacy, and thus their confidence in the digital world.

During the **2007-2013** period, the EU invested a total amount of **€334 million** in cybersecurity and online privacy projects from both the **7th Framework Programme** (FP7) and **the Competitiveness and Innovation Programme (CIP)**. In the privacy field, this investment supported in particular innovation in privacy enhancing technologies and in electronic identity management.

In addition, several projects in the field of cybersecurity dealt with privacy issues, for example by examining the privacy implications of advancing in security by means of biometrics.
Examples of successful projects funded under the 2007-2013 programming period include: PRIPARE, which delivered a handbook of methodological tools helping organisations comply with the principles that also underpin the new General Data Protection Regulation (e.g. "privacy by design"); ABC4Trust, which developed a system that puts users' electronic identities in their hands, and TABULA RASA, which worked on improving the security of biometric recognition systems.

Under the new Horizon 2020 Programme, the Commission has foreseen, for the 2014-2020 period, a total investment of **€500 million** in cybersecurity and privacy projects. This includes, for the 2014-2017 period, about **€37 million** specifically allocated to privacy and **€37 million** to cryptology (examples of ongoing projects include: Safecrypto, Pqcrypto, Hector, eCrypt, Heat).
Projects dealing with privacy matters can be found in two streams:

- Leadership in Enabling and Industrial Technologies **(LEIT)**: here are funded projects delivering building blocks, such as research on cryptography, that are key to deliver enhanced digital privacy.
- Societal Challenge "Secure societies – Protecting freedom and security of Europe and its citizens", where privacy is addressed under the Digital Security overall theme.

ISBN 978-00-00-00000-0, doi:10.2775/00000, NA-AD-14-001-EN-N