Briefing

EU Legislation in Progress

September 2017

European Parliament

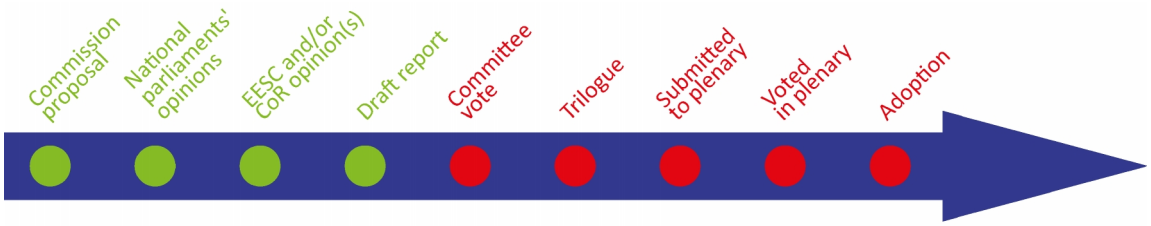
Reform of the e-Privacy Directive

OVERVIEW

In January 2017, the Commission tabled a proposal for a regulation on privacy and electronic communications which would replace the current 2002 e-Privacy Directive. The main objectives of the review are: enhancing security and communications confidentiality; defining clearer rules on tracking technologies such as cookies; and achieving greater harmonisation among Member States.

Stakeholders are divided on certain issues, including on the basic need for a new measure to protect confidentiality in e-communications. Some national parliaments have made comments on the proposal, and discussions are progressing in Council. In the European Parliament, rapporteur Marju Lauristin (S&D, Estonia) presented a draft report to the Civil Liberties Committee on 21 June 2017, and this is expected to be voted in October 2017.

Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)		
Committee responsible:	Civil Liberties, Justice and Home Affairs (LIBE)	COM(2017) 10 10/1/2017
Rapporteur:	Marju Lauristin (S&D, Estonia)	2017/0003(COD)
Shadow rapporteurs:	Michal Boni (EPP, Poland) Daniel Dalton (ECR, UK) Sophia in 't Veld (ALDE, the Netherlands) Cornelia Ernst (GUE/NGL, Germany) Jan Philipp Albrecht (Greens/EFA, Germany) Lorenzo Fontana (ENF, Italy)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Next steps expected:	Vote in committee	



EPRS | European Parliamentary Research Service

Author: Shara Monteleone

Members' Research Service

PE 608.661

EN

Introduction

One of the Juncker Commission's priorities is the completion of the digital single market (DSM), as the main objective of the European Commission's digital agenda, aiming to create the right environment for digital networks and services to flourish, by providing the right regulatory conditions. Reinforcing security and trust in digital services, which serves to create these conditions, requires strong European data protection and privacy rules to boost the EU digital economy and ensure fundamental rights protection. In line with the DSM strategy, which includes the revision of the e-Privacy Directive among its initiatives, the Commission published a proposal in January 2017 for a 'regulation on the respect for private life and the protection of personal data in electronic communications'. The aim is to reform the existing 2002 legislation to adapt the e-Privacy rules to the new technological reality, and to align them to the 2016 General Data Protection Regulation (GDPR). The objectives of the review are: enhancing communications security and confidentiality; defining clearer rules on tracking technologies such as cookies; and achieving greater harmonisation among Member States. The idea is to have the regulation adopted by 25 May 2018, when the GDPR enters into application, in order to provide citizens, companies and institutions with a consistent legal framework.[1]

Context

Both privacy and data protection are fundamental rights enshrined in EU primary and secondary law. Article 7 of the Charter of Fundamental Rights (CFR) provides for the right to privacy, stating that 'everyone has the right to respect for his or her private and family life, home and communications'. Article 8 of the European Convention on Human Rights (ECHR) also provides for the right to privacy. Under Article 52(3) CFR, the meaning and scope of the fundamental rights guaranteed in the Charter are to be given the same meaning as in the ECHR. The protection of natural persons in relation to the processing of their personal data is also a fundamental right, enshrined in Article 8 of CFR and in Article 16 of the Treaty on the Functioning of the EU (TFEU).[2] Article 8 CFR also states that personal data 'must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'. According to the case law of the European Court of Human Rights (ECtHR), the protection of personal data is a fundamental component of the right to privacy.[3]

The main current data protection and privacy instrument in EU secondary legislation is the Data Protection Directive (95/46/EC),[4] complemented by Directive 2002/58/EC (i.e. the **e-Privacy** Directive) as regards the confidentiality of e-communications.[5] The GDPR, which will replace the 1995 Data Protection Directive from 25 May 2018, contains general principles and rules to apply when entities in the private or public sector process personal data (e.g. conditions for lawful data processing, obligations and rights deriving from data processing and safeguards). The e-Privacy Directive also aims at avoiding unjustified limitations to free data flow, considered essential for innovation and competitiveness.[6] Accordingly, processing of personal data is allowed under certain conditions, providing the subjects of the data retain their right to a private life, freedom of expression, and other rights. This rights-based approach is closely related to self-determination and human dignity (as enshrined in Article 2 CFR).

General Data Protection Regulation (GDPR), core principles

Requirements for lawful data-processing (collection, analysis, storage, etc.) include:

- data-subject's consent or other legal grounds, such as the existence of a contract or of a legal obligation for the controller to respect, or controller's overriding legitimate interests.
- specified, explicit and legitimate purposes, and for no longer than necessary;

Rights of the data-subject include:
- the right to be informed in a clear way that personal data are being processed;
- the right, in some cases, to object to the processing on legitimate grounds;
- the right not to be subjected to an automated decision intended to evaluate certain personal aspects, such as performance at work or creditworthiness.

Moreover:

- the subject or entity responsible for data processing (data controller) shall respect data confidentiality and security; including notifying both individuals and the responsible authority in cases where data is accidentally lost, or unlawfully accessed ('breach notification').
- increased responsibility and accountability for those processing personal data may imply the requirement to designate a Data Protection officer (DPOs) and carry out an impact assessment. Technology developers have to comply with the '**data protection by design**' and by **default** (i.e. 'to embody' data protection requirements in a product or service at an early stage and to program the most privacy-friendly settings).
- Individuals can file an application with national Data Protection Authorities, which may prohibit data processing (besides other judicial remedies).

The Commission considers the alignment of e-Privacy rules with the GDPR as essential to ensuring a consistent EU framework. The update to the legislation also appears triggered by the advances in digital technologies of the last decade. Communications today do not only take place via traditional telecommunications services (e.g. phone calls, SMS), but more often go through 'over the top' (OTT) services, including internet-based messaging, Voice over IP (e.g. Skype, Whatsapp), which are not covered by current e-Privacy rules.

Existing situation

At present, protection of privacy in electronic communications is provided by Directive 2002/58/EC (e-Privacy Directive (e-P Directive), as modified by Directive 2009/136/EC, also known as the **Cookies** Directive.[7] The e-P Directive complements the 1995 General Data Protection Directive and provides specific rules for e-communications services, in particular on: **confidentiality** of e-communications and related data, of both natural and **legal persons**; unsolicited communications (**spam**); network and services security; **data breach** notifications; limited storage of **traffic** and **location** data, as well as rules on **cookies**.[8] The e-P Directive's aim was to harmonise national rules on e-communications confidentiality, but the situation appears far from harmonised, with divergent approaches in the Member States and a consequent lack of an equivalent level of protection for European citizens, and uncertainty for companies (especially cross-border).[9]

Regarding the **scope** of the current e-P Directive, its obligations to ensure e-communications confidentiality covers **only** traditional telecom operators (the main providers collecting e-communications data at the time of adoption). With the convergence of media and technological innovation, and different treatment of new – but functionally equivalent – e-communication services ('over the top' and various other information society services) no longer seems justified. In addition, the e-P rules apply to

publicly available e-communications services in public networks, leaving aside the debated cases of publicly accessible **private** communications networks (such as wifi connections in airports).[10]

The e-P Directive limits the collection and storage of **traffic** data regarding communications to that necessary for the transmission of communication or for billing purposes; in other cases (e.g. for marketing purposes), the prior consent of users is required, as is the case for **location** data. The directive does not consider other communications-related data.[11]

As for other obligations, (telecoms) providers shall adopt technical and organisational measures to ensure the **security** of their services. They also have data **breach notification** obligations towards their subscribers. It should be noted that the GDPR has extended these obligations to apply to any provider.

Regarding **tracking tools** and means to access data stored in users' terminal equipment, such as **cookies**, under the current directive their use is allowed with the informed consent of the interested user. As mentioned below, studies have confirmed that the **cookies** rules, as introduced by the 2009 revision of the e-P Directive, fail to achieve their goal (to enable users to make a real choice and give informed consent), causing, to the contrary, the irritation of users called to repeatedly consent to the use of cookies and faced with 'cookies walls'.[13]

Regarding the **national authority** responsible for enforcing the e-P rules, the directive leaves the choice to the Member States, with consequent uncertainty and overlaps, as the body responsible may vary from country to country (data protection authority or telecoms regulator).

The reform put forward in January 2017 clearly builds on this directive, but introduces **changes** in view of ensuring greater harmonisation of e-privacy rules in line with technological developments. The ambition is to address the needs of both consumers and businesses, although divergent positions are emerging.

Cookies

A cookie is information saved by the user's web browser. When visiting a website, a site might store cookies to recognise the user's device in the future upon their return to the page. By keeping track of a user over time, cookies can be used to customise a user's browsing experience, or to deliver targeted advertisements. First-party cookies are placed by the website visited to make experience on the web more efficient (e.g. they help sites remember items in the user shopping cart, or log-in names). Third-party cookies are placed by e.g. an advertising network to deliver ads to the online user, in the visitor's browser with the purpose of monitoring (through identifiers) their behaviour over time.

Source: European Commission, impact assessment on the e-Privacy proposal.[12]

Parliament's starting position

The European Parliament (EP) called for the revision of the e-P Directive on several occasions, and in particular in its resolution 'towards a digital single market act' (rapporteurs: Evelyne Gebhardt, S&D, Germany, and Kaja Kallas, ALDE, Estonia), of 19 January 2016, which urged the European Commission to ensure the consistency of new e-Privacy provisions with the GDPR.[14]

The issue was also debated at conferences organised by the EP (e.g. the high level conference on protecting online privacy held in 2015 by the Civil Liberties Committee (LIBE) and by Science and Technology Options Assessment Panel of the EP (STOA)).

European Council starting position

In its conclusions of December 2016, the European Council called on the EU legislators to remove remaining obstacles within the single market, including those hampering the free flow of data. In its June 2017 conclusions the European Council highlighted the importance of an ambitious digital vision for Europe, which requires the implementation of the DSM strategy in all its elements. Safeguards for the protection of privacy are explicitly mentioned only when it calls for addressing at the EU level the challenges posed by systems such as end-to-end encryption to counter-terrorism authorities.

Preparation of the proposal

In 2015, the European Commission published the results of an external study, commissioned to assess the transposition, effectiveness and interaction of the e-P Directive with the (at the time) proposed GDPR.[15] The final report recommended, inter alia: to extend e-P rules to **publicly** accessible **private** networks, including rules on traffic and location data (to cover ambiguous cases such as airport wifi); to increase clarity and strengthen requirements for the use of cookies and for unsolicited communications and to replace the directive with a regulation.

The need for reformed e-Privacy rules emerged in particular from the public consultation carried out by the Commission between April and July 2016, to which 421 stakeholders responded. The results are a 'mixed picture', with quite diametrically opposed positions between citizens, authorities and industry representatives.[16]

In parallel, a Eurobarometer survey was conducted in July 2016. The data collected showed that more than half of the respondents use mobile phones daily and use internet for instant messaging; the majority consider the confidentiality of their emails and online messaging as important and that cookies are to be used only with their consent; most respondents change the privacy settings of internet browsers to protect their data, and would like service providers to make a range of protection measures available.

The Commission also carried out an ex-post regulatory fitness and performance programme (REFIT evaluation) of the e-Privacy Directive. From this evaluation, it follows that while the principles of the directive remain sound, considerable technological and economic developments have since taken place in the market. Consumers and businesses increasingly rely on new internet-based services enabling inter-personal communications, such as 'voice over IP' (VoIP), instant messaging and web-based e-mail services (e.g. Whatsapp, Facebook, Messenger, and Skype). These 'over the top' (OTT) communication services are not covered by the current e-P Directive. According to the Commission's evaluation, some of the provisions appear redundant, primarily due to changes in legislation on technology. This is the case for the **security** requirements and the obligation to **notify** personal data breaches, which are covered by provisions in the GDPR. Problems were identified in particular with regard to:

- the limited transparency regarding cookies used for tracking, and the shortcomings related to the common method used to seek consent – 'take it or leave it' banners, or 'cookies walls' (Article 5.3 of the e-P Directive);
- the scope of the provision under Article 5.3 (confidentiality of communications) was considered both too wide (it should not include first party analytics), and too narrow (it should include all tracking techniques).

The evaluation confirmed the EU added value of the e-P rules. However, adjustments appeared necessary to ensure consistency with the GDPR.

In parallel to the ex-post evaluation of the e-P Directive, the Commission published an impact assessment (IA) on the proposal for the new regulation. Among the various options available to achieve the objectives of effective confidentiality of e-communications and harmonising/updating the legal framework, the preferred option (taking into account the different stakeholders' opinions) was deemed to be that offering a **measured** reinforcement of privacy and harmonisation with balanced measures, without imposing an excessive burden on the relevant stakeholders. The IA was evaluated positively in the European Parliamentary Research Service (EPRS) initial appraisal, which, however, considers that monitoring and evaluation indicators could have been developed more clearly. An implementation appraisal was also published by EPRS on the 2002 e-P Directive, which provides an overview of the materials and research available on the application and effectiveness of the same directive.

The changes the proposal would bring

The announced goal of the reform is to get a coherent and up-to-date framework capable to strike the balance between industry's interests (ensuring free movement of data and e-communications services within the EU) and users' rights to privacy and data protection. Although these two rights are intertwined, they are recognised autonomously in the CFR (respectively in Article 7 and 8).[17] The proposal seems based mainly on Article 7, as respect for the privacy of personal communications is an essential dimension of the right to private life (Recital 1). The ambition to safeguard privacy in in the field of electronic communications not specifically covered by the GDPR, would justify the proposed reform.[18]

A regulation instead of a directive

The Commission proposed a **regulation,** instead of a new directive, to replace the current rules, claiming that full harmonisation can best be achieved through this directly applicable legal instrument. Therefore, as the e-Privacy Directive currently complements the 95/46/EC Data Protection Directive, the proposed e-Privacy regulation will particularise and complement the GDPR. A regulation should ensure consistency with the GDPR, as well as legal certainty for users and businesses, by avoiding divergent interpretation in the Member States, although some flexibility is envisaged. In particular, Article 11 contemplates the possibility for Member States to restrict, through a legislative measure, the scope of the obligations and rights provided for in the same proposal when it is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23 GDPR (e.g. national security, defence, public security, prevention, investigation of crimes etc.).[19]

The Commission claims that the e-Privacy proposal will contribute to making the level of protection of privacy and data protection more effective with regard to e-communications (personal) data. As it is meant to complement the GDPR, containing the general principles and rules, the latter always applies, except when the e-P *lex specialis* provides differently.[20] The proposal refers in general to the GDPR for definitions and core concepts and updates previous rules (e.g. on traffic and location data), seeking to avoid duplication. This is reflected in the fact that some provisions of the current e-P Directive have been deleted in the proposal. However, several **issues** in terms of compatibility and possible overlap with the GDPR (and with the upcoming e-communications code) seem to persist, requiring further reflection and discussion.

Wider scope

Regarding the content, one of the changes introduced with the reform concerns the material and territorial **scope** of the e-Privacy rules, which, in light of the new market and

technological reality, cover a wider range of services entailing data processing. It applies to the provision of e-communications services to **end-users in the Union**, irrespective of whether the end-user is required to pay for the service. Providers outside the EU have to appoint a representative in the EU.

The proposal applies not only to traditional telecom providers, but also to other market-players (e.g. information society service providers) providing internet-based services, such as VoIP, instant messaging applications and web-based emails (OTTs), with the aim of ensuring a level playing field for companies. It applies to e-communications data processing carried out in connection with the provision and use of e-communications services **and** to information related to the terminal equipment of end-users.

Differently from the directive, the regulation would apply its core rules on respect of confidentiality to both the **content** and **metadata** of communications. With the advances and sophistication of new e-communications technologies, metadata, commonly defined as external e-communication data, proves able to reveal more detailed information about individuals (preferences, habits, life style) than the mere 'traffic data related to communications' (as stated in the e-P Directive). It is worth noting that traffic and location data are a type of metadata,[21] which, as regards the new e-communications, are deemed to include more information about an individual's life than ever before. Nevertheless, discussions on whether a distinction between content and metadata should be retained are ongoing.

In addition, **issues** related to the scope of the new regulation, as well as its definitions and exceptions, are currently under discussion. The mere question of whether it is appropriate (or not) to adopt an additional legislative instrument, other than the GDPR, for e-communications and of its consequences for industry and citizens is not uniformly addressed, as has emerged in current debates.

Other major aspects of the review include:

Technological neutrality and new rules on tracking tools (cookies)

- a focus on security and **confidentiality of (all) e-communications, regardless of the technology or service** used, by extending, as previously mentioned, the related obligations to a broader range of providers, to include OTTs;
- new rules on **tracking technologies** (including, but not limited to **cookies**). Firstly, the collection of information from the end-user's device is allowed only under specific conditions, e.g., for the sole purpose of carrying out the transmission of an electronic communication, **or** with the end-user's consent, **or** if it is needed to provide a service requested by the end-user (Article 8.1). The collection of data **emitted** by terminal equipment, e.g., via WIFI, to enable connection to another device or to a network (Article 8.2) is allowed for the purpose of, and the time necessary for, establishing a connection, **or** if a clear and prominent informative notice is displayed (according to GDPR Article 13). The latter seems to suggest that user device location tracking is allowed without consent.[22]

Privacy settings

In line with the GDPR, when provided, **consent** must be freely given and unambiguous, but can be expressed by a clear affirmative action. To this end, the new rules provide for the possibility that the consent is given at the level of **browser settings**, when technically possible and feasible (Article 9), to avoid the consent fatigue caused by current pop-up banners. Article 10 refers to **options for privacy settings** that browsers should offer to enable users to prevent third parties from tracking online data related to their terminal

equipment, deemed a part of their private sphere (Recital 20). This seems to imply that browsers will be required to include this feature in all new software.

Unsolicited communications

To enhance protection against unsolicited communications (**spam**), the main principle is that communications used for direct marketing are allowed under user consent (opt-in), except for existing customers contacted via email for similar products or services, for whom an opt-out is guaranteed. Member States may, however, legislate to provide an opt-out regime for direct marketing that **uses voice-to-voice calls** (Article 16).

Consistent enforcement across Europe and sanctions

- More uniform enforcement rules addressing the issue of **fragmentation of legislation** across Europe seem necessary, as Member States apply the existing e-P Directive in different ways. Fragmentation is expected to diminish with the adoption of the proposed regulation, which will be directly applicable. Moreover, the Commission aims at achieving more consistent enforcement of e-Privacy rules by assigning the related supervisory powers to the national independent **authorities already competent** to enforce the GDPR. So far, in fact, the authority responsible for the enforcement of e-Privacy rules may differ from country to country, in some cases being the data protection authority, and in others the telecoms regulator.
- **Tougher sanctions** in cases of infringement of the main e-Privacy rules, with fines up to 4 % of the total worldwide annual turnover.

Advisory committees and other bodies

The European Economic and Social Committee (EESC)

The EESC discussed the proposal in the Transport, Energy, Infrastructure and Information Society (TEN 631) section meeting of 14 June 2017 and adopted its opinion in plenary on 5 July 2017 (rapporteur: Laure Batut, Workers – Group II, France,). Besides regretting that the proposal is voluminous and entangled, the EESC recommends, inter alia, not to diminish the established protection of the GDPR in favour of industry interests, to allow consumers to bring class actions before the courts, and to take into account the internet of things (IoT), which is most intrusive of private life; priorities should include user education , as well as anonymisation and encryption. In addition, the EESC published a study on the ethics of big data in 2016, containing insights relevant for the e-Privacy reform, including recommendations to develop a European certification system for companies.

The Committee of the Regions decided not to issue an opinion.

The Article 29 Data Protection Working Party

The independent European advisory body on data protection, the Article 29 Working Party (Art29WP), representing the European data protection authorities (DPAs) and set up under Article 29 of Directive 95/46/EC, released an opinion on the proposal for an e-Privacy regulation on 4 April 2017. Although the Art29WP welcomed some of its main aspects (the choice of a regulation, the extension of the confidentiality obligations to OTT providers, the updated rules on online tracking), some remaining **concerns were expressed**. In particular, the Group of DPAs noted four points of concern related to: 1) **wifi tracking**; 2) **content and metadata analysis**; 3) **tracking walls** (calling for explicit prohibition); and 4) **privacy by default** (in the privacy settings of terminal equipment and software). In brief, in the Art29WP view, the proposed regulation should **provide an equal or higher level of protection than the GDPR, not lower**.

The European Data Protection Supervisor (EDPS)

Consultation of the **EDPS** is mandatory, and the EDPS also provided an opinion, which is in line with the Art29WP opinion. Welcoming the Commission's attempt to provide for the necessary comprehensive protection of e-communications, the EDPS, however, called for smarter, clearer, and stronger rules. The EDPS pointed out the risks of gaps in protection that may emerge from this complex proposal (which, for instance, would split communications data into different types associated with different levels of confidentiality and exceptions). The EDPS also expressed concern as regards the intention to base the definitions of the e-P proposal on the upcoming European e-communications code's market-oriented definitions, and suggested that a set of specific definitions is included. The need to protect e-communications from unlawful online tracking (e.g., without freely-given user consent) was also emphasised. Other issues may need further clarification as a consequence of the e-P regulation's complementarity with the GDPR (which also covers the protection of communications confidentiality), including the critical issue of user consent.

National parliaments

A number of national parliaments have examined the proposal, without raising any subsidiarity objections. By end of June 2017, contributions from several national chambers (Portuguese Parliament, Czech Chamber of Deputies and Senate, Spanish General Courts, Netherlands Senate, German Bundesrat and Italian Chamber of Deputies) were received.

Stakeholders' views

This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all the different views on the proposal. Additional information can be found in related publications listed under 'EP supporting analysis'.

Stakeholders' positions on the proposal may be said to be quite divergent among citizens, public authorities and industry representatives.

The European Digital Rights (EDRI) association provided its own proposal for amendments, suggesting, inter alia, specific definitions of concepts such as e-communications services and metadata, and that the new regulation should not refer to the upcoming e-communication code for definitions not contained in the GDPR. EDRI suggests that e-communications data confidentiality should be guaranteed whether in transit or stored (e.g. on the 'cloud'). The association calls for strong reliance on consent or on other legal grounds for further processing (Article 5-6), e.g., when it is **strictly** necessary for the transmission of communications; and asks for total ban on 'take it or leave it' processing (where the user is denied access to a service on the grounds that they do not provide consent to data processing), and for fine-grained control through browser settings (specific, not generic, consent for each service).

The European Consumer organisation, BEUC, welcomed the reform, but evidenced some critical points, such as: the possibility to track user location and movements without consent (Article 8.2); the lack of privacy due to default settings (Article 10); lack of provision on collective redress; and on children's privacy.

Similar considerations were voiced by Access Now, which calls for higher protection of individual's rights, and argues that the new regulation should not only uphold the level of protection afforded by the GDPR but exceed it 'to level the playing field for the users'.

Statewatch claims that the Council may try to introduce a general data retention obligation for e-communications providers in the e-P proposal, bypassing the CJEU judgments.

Industry representatives such as FEDMA, instead, voiced their aversion to the proposal, arguing the GDPR is sufficient to protect consumers. In particular, they consider its negative effects on online advertising and modern marketing.

DigitalEurope, the association of information technology companies, was sceptical about the benefits that e-P reform would bring, which in its view, will hamper European companies' ability to benefit from data-driven innovation and therefore undermine the development of Europe's digital economy. The association urges alignment of the e-P proposal with the GDPR, including as regards sanctions, to avoid their 'disproportionate extension', as well as with regard to the legal bases for data processing other than consent (e.g. **legitimate interest** of the data controller). However, it calls on the co-legislators not to rush negotiations but to evaluate properly the implications of the reform for companies.

The concerns of telecommunications and mobile associations ETNO and GSMA are reflected in a joint statement calling for greater flexibility to use data responsibly and to permit (compatible) further processing.

Legislative process

The legislative proposal (COM(2017) 10) was published on 10 January 2017, under the ordinary legislative procedure.

Parliament

Within the European Parliament, the proposal was assigned in March 2017 to the Civil Liberties Committee (LIBE). On 11 April 2017, the LIBE Committee held a hearing to discuss the main issues with experts and to consider possible improvements.

The draft report was presented by rapporteur Marju Lauristin (S&D, Estonia) in LIBE on 21 June 2017, with amendments to be tabled by 14 July 2017. The rapporteur shares the objectives put forward in the Commission's proposal. However several changes are proposed in the draft report, which focuses on **consent** (when processing is not 'technically strictly necessary'), as the main legal ground for exceptions to the core rules on e-communications confidentiality (Article 6), and of terminal equipment (Article 8). In particular, the report stresses: the need to apply the stricter GDPR conditions (e.g. privacy by design and by default) to the processing of data on or stored in users' terminal equipment, including in cases of **machine-to-machine** interaction and of connection with other devices or network (e.g. wifi, hotspots), if related to users; as well as that **privacy settings options** should be easily accessible and changeable. The rapporteur also urged 'smooth and rapid cooperation' between the national data protection authorities and other enforcement bodies in the field of consumer protection (e.g. regulatory authorities established by the forthcoming e-communications code).

The more than 800 amendments (in total) submitted in July reflect the different opinions of MEPs on some critical issues, such as: the admissibility (or not) of legitimate interest as a legal ground for further processing; opt-in vs opt-out regimes; same vs different rules on content and metadata; and the regime applicable to wifi-tracking.

The Industry, Research and Energy (ITRE) Committee, the Internal Market and Consumer Protection (IMCO) Committee, and the Committee of Legal Affairs (JURI) will provide opinions, while the Committee on Employment and Social Affairs (EMPL) decided not to give an opinion.

The vote on the report in LIBE Committee, the Parliament's position (first reading), and the mandate for entering into negotiations with the Council are expected for October 2017.

An in-depth assessment of the proposal has also been conducted by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, which notes the considerable improvements, but has also identified shortcomings. The study recommends, inter alia, that location tracking (via wifi) only be allowed upon user consent, that browsers are set to privacy by default, and that 'take it or leave it' choices (tracking walls) are banned, at least in some cases.

Council

Within the Council, under the Maltese Presidency, the proposal was assigned to the Telecommunications and Information Society working party (TELE WP), which completed a first examination of the proposal. Member States generally welcomed the proposal's aims, although they also requested adjustments. The Council published its progress report on 19 May 2017, summarising some of the issues raised by the delegations, including: the interaction of the new rules with the GDPR and the upcoming e-communication code; the scope of the new regulation (extension to OTT services and to 'ancillary services'); the breadth of the provision on confidentiality of e-communication data. Progress made on the proposal was presented to the ministers at the Transport, Telecommunications and Energy (TTE) Council of 9 June 2017. As detailed discussions still seem to be required, delegations considered the proposed date for the entry into force of the new regulation of 25 May 2018 difficult to achieve. The Estonian Presidency, which includes among its priorities 'a digital Europe and free movement of data', intends to advance on the e-Privacy proposal, as a significant complement to the other digital files on the agenda. Some of the outstanding issues include the interplay with the GDPR and the breadth of exceptions applicable to cookies. Finally, at the Justice and Home Affairs Council of July in Tallinn, the Presidency invited delegations to exchange views regarding the e-P proposal as an option to address the data retention issues arising from the CJEU case law,[19] in light of the Article 11 proposal (e.g. whether enforcement authorities would be permitted to access data processed by OTT).

EP supporting analysis

Schrefler, L., Review of the ePrivacy Directive, implementation appraisal, EPRS, European Parliament, February 2017.

Kononenko, V., with Parise, R., Respect for private life and protection of personal data in electronic communications, initial appraisal of a Commission impact assessment, EPRS, European Parliament, April 2017.

Policy Department C: Citizens' rights and constitutional affairs, study for the Civil Liberties, Justice and Home Affairs Committee, An assessment of the Commission's Proposal on Privacy and electronic Communication, Directorate General for Internal Policies, European Parliament, May 2017.

Policy Department C: Citizens' rights and constitutional affairs, study for the Civil Liberties, Justice and Home Affairs Committee, Big data and smart devices and their impact on privacy, Directorate General for Internal Policies, European Parliament, 2015.

- Monteleone, S., Golden eye, who rules tomorrow's Europe, EPRS, European Parliament, 2016.

Other sources

Respect for private life and the protection of personal data in electronic communications, European Parliament, Legislative Observatory (OEIL).

Endnotes

[1] In parallel, the Commission, also proposed a regulation on the processing of personal data by the Union institutions, which seeks to be consistent with both GDPR and the e-privacy regulation.

[2] Article 16 TFEU provides that the rules on the protection of individuals with regard to data processing by the EU and Member States acting within the scope of EU law are to be laid down following the ordinary legislative procedure.

[3] See for instance, *S and Marper v UK*, in the context of criminal justice.

[4] This directive amplifies the principles contained in the Council of Europe Convention no 108/1981.

[5] Directive 2002/58/EC (e-Privacy Directive) is part of the 2002 EU telecoms package.

[6] See European Parliament, Directorate General for Internal Policies, Policy Department A, Economic and Scientific Policy, Study for the Committee on Industry, Research and Energy, Data Protection Review: Impact on EU Innovation and Competitiveness, 2012.

[7] While Directive 95/46/EC protects only the rights of natural persons, the e-P Directive also protect legal persons.

[8] See Article 29 Working Party opinion 4/2012 on cookie consent exemption.

[9] See the results of the Study SMART 2013/0071 (2015), which also contains country reports.

[10] See European Parliament, EPRS, implementation appraisal, Review of the ePrivacy Directive, February 2017.

[11] See Art29 WP cit., where it criticised the e-P Directive for the lack of clear distinction between **communications and related traffic data** and **traffic data** per se.

[12] See also Article 29 Working Party, opinion 2/2010 on behavioural advertising.

[13] See, Article 29 Working Party, opinion 03/2016 on the evaluation and review of the e-Privacy Directive and EDRI, e-Privacy revision: An analysis from civil society groups.

[14] See also recent EP resolution of 15 June 2017 on online platforms, where the EP called on 'the Commission and the Member States to take the necessary measures to ensure full respect of citizens' rights to privacy and to protection of their personal data in the digital environment'.

[15] SMART 2013/0071, followed by other two external studies conducted by Deloitte (SMART 2016/0080) and Ecorys-TNO (SMART 2013/0019).

[16] However, as stressed in the EPRS implementation appraisal, even within the same category of stakeholders, there is not necessary a uniform position, e.g. industry including traditional telecoms and OTTs.

[17] See, inter alia, D. Wright & P. de Hert (eds), Enforcing Privacy, 2016, with further references.

[18] See G. Buttarelli, The Commission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation Dedicated to ePrivacy in the European Union? EDPL 2, 2017.

[19] In this regard, in *Tele2 Sverige/Watson*, the Court of Justice of the European Union, (also in view of the annulment of the Data Retention Directive by its 2014 judgment), clarified that Article 15 of the current e-Privacy Directive 'must be interpreted as **precluding** national legislation which, for the purpose of fighting crime, provides for **general and indiscriminate retention** of all traffic and location data of all subscribers and registered users[...]'.

[20] The issue of the relationship between future e-P regulation and GDPR (and the meaning of *lex specialis*) is under debate as it emerges, for instance, from the amendments and from the draft opinion of the JURI Committee.

[21] See definitions contained in the proposal for e-P regulation Article 4.2 (c).

[22] See EP, Directorate General for Internal Policies, Policy Department C: Citizens Rights' and Constitutional Affairs, Study for the LIBE Committee, An assessment of the Commission's Proposal on Privacy and electronic Communication, May 2017.

Disclaimer and Copyright

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

First edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.