Computer & Communications Industry Association

Tech Advocacy Since 1972

CCIA Position Paper on the proposed E-Privacy Regulation

The Computer & Communications Industry Association ('CCIA Europe') welcomes the opportunity to present its views on the Commission's proposal for a Regulation on Privacy and Electronic Communications ("EPR").

CCIA Europe represents a wide range of innovative companies in the computer, Internet, information technology, and telecommunications industries which all put user trust at the centre of everything they do. Ensuring privacy and the confidentiality of user communications is paramount to gain and retain user trust for our Members. We therefore very much welcome the objectives which the European Commission is pursuing with this proposal.

However, we are concerned that the proposed ePrivacy rules may only tip the scale towards sheer prescriptiveness, without due consideration of the technical and market realities of modern digital technologies. More importantly, the proposal significantly departs from the context- and risk-based approach of the General Data Protection Regulation, creating overlaps and raising legal tensions across multiple aspects of both texts, and without necessarily bringing any added value in terms of privacy, confidentiality of communications, or user control.

Although many of its provisions may be well-intentioned, we recommend introducing several substantial changes to shift the approach of the proposal towards a more meaningful, outcome-oriented privacy and confidentiality regime without hurting digital growth and innovation in Europe. To this end, we invite lawmakers to consider the following points:

- **The principle of confidentiality of communications and permitted processing should only apply during the transmission of electronic communications.** The processing of personal data in electronic communications before and after their transmission should be subject to the General Data Protection regulation;

- **Third-party processors should be allowed to process electronic communications data** on behalf of electronic communications and network service providers;

- Service providers should be able to **process communications on the basis of additional legal grounds, including legitimate interest**;

- **The ability for Member States to restrict the principle of confidentiality** for public interest purposes **should be limited to what is strictly necessary in a democratic society.**

- The **consent regime** to process communications data, and store, access and process personal data on end-user's terminal equipment **should remain principle-based, and consistent with the General Data Protection Regulation**;

- The proposal should introduce **additional legal grounds to access and process data stored and emitted from end-user's device**, including legitimate interest;

- The **proposed EPR should remain technology neutral** and avoid erecting all kinds of software as gatekeepers of online content and enforcers of EU's consent regime;

- **Access to online content and services should be made conditional upon cookie acceptance**, in line with the existing ePrivacy framework.

On a more general note, CCIA Europe recalls that many of the processing operations which would be subject to the proposed EPR will, at a minimum, fall under the purview of the General Data Protection Regulation. We therefore invite lawmakers to take stock of what the GDPR has achieved, and to what extent additional rules rules are necessary to ensure meaningful privacy and confidentiality of communications.

Ensuring secure and seamless communications online

1. Allow processing of communications before and after transmission

The proposed Regulation rightfully prohibits the tapping, listening and other forms of interception of communications during their transmission. This prohibition is must-have to ensure that private communications remain confidential and sustain trust in online communications.

However, the proposal extends this prohibition well beyond the transmission stage, capturing all processing operations occurring before and after their transmission[1]. This would leave electronic communications service providers ('ECS') with very limited scope to process content and traffic data[2] and would undermine their ability to provide essential add-on services and functionalities.

Today, some of these services are taken for granted by citizens, public and private organisations alike. For instance, processing of data is required to perform security threat detection, spam filtering, spell-checking, file attachment checking. Cross-device synchronisation, virtual assistants, and follow-up suggestions also require processing of communications data before and after transmission to provide seamless and richer end-user experiences.

Recommendation: The general prohibition of interference into end-users' communications and the exceptions thereof (Articles 5-7) should only apply during the transmission phase i.e. from the time the

[1] See for instance Article 5 which reads: "any interference (...) such as by (...) *storing*, (...), *scanning* or other kinds of (...) *processing* of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation."

[2] As per Articles 6 and 7.

data leaves electronic communications service providers' infrastructure to the moment it reaches the recipient's service provider's servers. Since all communications data qualify as personal data[3], **any processing operations occurring before and after the transmission should comply with the General Data Protection Regulation**. This will avoid disruption of online communications services and leave breathing room for innovation without compromising on data protection standards.

>> see suggestions for amendments to Articles 5 and 2.

2. Allow trusted third-party service providers to process communications

Under the proposal, only electronic communication service (ECS) providers and electronic communication network (ECN) providers can process communications data. Any other service providers would not be able to process communications data[4].

This approach would jeopardise the provision of many communication services featuring or built on third party services which do not qualify as ECS or ECN under the proposed Electronic Communications Code ('EECC').

For instance, an ECS provider may use cloud-based network security services to monitor incoming traffic onto its customers' dedicated servers, detect botnets and DDoS (Distributed Denial of Service) attacks. The same ECS provider may also use third-party remote infrastructure (i.e. Infrastructure-as-a-Service, or 'IaaS') to build and host their VoIP and instant messaging services. Under the proposal, all these essential third-party services would have be developed, built, and implemented in-house which would considerably drive up costs for any ECS. This would severely negate the benefits of cloud-based models (economy of scale and deployment capabilities), and ultimately prevent the entry of new European players in the global online communications markets.

Recommendation: To avoid discontinuation of existing online communication services and to leave breathing room for new services to develop, we urge lawmakers to **extend the scope of permitted processing of communications to all trusted and essential third-party providers.**

>> see suggestions for amendments to Article 6

3. Introduce additional legal grounds for processing communications data

Respect for the confidentiality of end-users' communications is both a fundamental right and a beacon of customer trust for electronic communications service providers. Our Members therefore take the confidentiality of their customers' communications very seriously. Unfortunately, **the proposal fails to achieve its intended purpose** by erecting consent as the sole token of confidentiality and enabler of end-user control.

[3] See section 2.1 of the proposal explanatory memorandum, which states that "an electronic communication involving a natural person will normally qualify as personal data" (page 4). See also Article 29 Working Party opinion 01/2017 which recalls CJEU case-law on the extensive definition of personal data and asserts that "communications data generally are personal data" (page 27). See also more broadly Article 29 Working Party Opinion 4/2007 on the concept of personal data.

[4] Article 6(1)-(3) only allow "providers of electronic communications networks and services" to derogate from the general prohibition in Article 5.

a. Differentiating “confidentiality” from “sensitivity”

The proposal provides little to no possibility for ECS providers (and their third-party service providers) to process communications data unless end-users have given their consent (under Article 6(2) and (3)). This is based on the assumption that communications data are *inherently* sensitive and that the EPR should therefore mirror the consent derogation to process sensitive data under the GDPR.

We believe that ***context* determines whether communications data is sensitive or not**. **In other words, processing communication content and metadata may not *always* or *by default* represent a high risk to the users' fundamental rights**. This is in line with the existing case-law[5] and the General Data Protection Regulation on the definition of “special categories of personal data”[6]. More practically, the sensitivity of the data may vary depending on the very content and the degree of identifiability of the communications. Conversely, in some cases, content data would arguably not provide any personally identifiable information if the description of the communication (i.e. metadata) is absent.

Ensuring the confidentiality of communications is critical to maintain trust online. That being said, distinguishing the notion of “sensitivity” from “confidentiality” allows lawmakers to move away from a static derogation based on consent to a dynamic regulatory environment designed to achieve meaningful confidentiality of communications.

b. Consent as the sole legal basis would disrupt service continuity without necessarily ensuring confidentiality

By over-relying on consent and prohibiting further processing for compatible purposes, the proposal fails to take into account the technical realities of modern communications technologies. In doing so, the **proposal risks jeopardising the provision of existing and new services citizens and organizations have come to expect in an increasingly connected world, without necessarily ensuring confidentiality**.

Consent - especially “all party” consent under Article 6(3)(b); and a consent standard that is otherwise different from that of the GDPR - could be an impossible threshold for providers to meet without necessarily guaranteeing the confidentiality of communications. An overreliance on consent is also impractical for the users, as we have experienced with the cookie-banners over the last few years.

Consider the provision of an email service as an example. Under the current proposal, the provider would be compelled to request all end-users involved in the communication to consent, including in the case of “abusive”

---

[5] See joined cases C-203/15 and C-698/15 and joined cases C-293/12 and C-594/12. All cases assessed the validity of national and EU laws mandating general and indiscriminate retention of certain communications data (traffic and location data) for the purpose of investigation, detection and prosecution of serious crimes. In this context, the Court highlights “*that data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained (...)”* (para. 99 of the C-209/15).

[6] Communications data is not included in the exhaustive list of *inherently* sensitive data as defined in Article 9 and Recital 51 of the GDPR. *Inherently* sensitive data only specifically includes “data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited”.

use of the service. Because email services are interoperable by nature and that the sender's service provider will often have no contractual relationship with the recipient(s), service providers would necessarily require the processing of metadata (in this case, the email addresses of the sender or recipients) to direct the consent request to the relevant user(s). This processing operation alone would however be unlawful since consent can only be valid *prior* to the processing[7]. In other words, ECS providers would be compelled to ignore the conditions for consent in order to request consent. The problem would further exacerbate in cases of forwarded emails.

Even simple consent can be challenging, for example, in the case of automated messaging, like booking confirmation.

A consent-only solution for the processing of communications content and metadata would create unnecessary bottlenecks for the provision of services that end-users have requested, and without ensuring confidentiality of their communications.

Lastly, consent withdrawal notification under Article 9(3) would ignite a wave of notification every 6 months to end-users for each of the electronic communications service they use, from instant messaging services to email services, and any other services caught in the scope of the new E-Privacy rules. We strongly warn lawmakers about the unprecedented negative consequences that this would have on end-users' daily usage of such services. This provision also departs from the consent regime established in GDPR which does not require a six-month renewal[8], and it ignores existing obligations have under the GDPR, in particular privacy-by-design measures enshrining the principles of data minimisation, purpose limitation, and storage limitation[9].

We call on lawmakers to further consider the practical implementation that such a requirement would entail for both end-users and ECS providers.

c. Achieving confidentiality and control of end-users' communications beyond consent

We are convinced that the ability for service providers to **process metadata *and* content data based on contractual guarantees** and **legitimate interest and** their ability to **further process** such data are **essential to ensure seamless and secure communications**.

We recall that the use of legitimate interest as a legal ground for processing requires the service provider (or "data controller") to foresee the scale and type of the data and the frequency of the expected processing, identify specific interests and purposes related to the envisaged processing, anticipate the expectations of the end-user, map out the implications for the end-users that the processing may entail, and calibrate and apply appropriate technical and organisational measures to mitigate potential risks to the fundamental rights and interests of end-users (or "data subject").

Contracts may also provide for additional confidentiality and control measures to reflect the specific needs of the end-user(s), particularly for public or private legal entities.

---

[7] As per the Article 29 Working Party guidance on consent (e.g. Opinion 15/2011 and the 2017 draft guidelines on consent (WP259)).

[8] See the conditions for consent under Article 7 of the GDPR.

[9] See Article 25 together with Article 5 of the General Data Protection Regulation.

Further processing also entails a detailed ex-ante review of the compatibility of the initial and subsequent purposes of processing, along with the implementation of appropriate safeguards.

Finally, and regardless of the ground of processing, we believe that **transparency requirements and end-user rights** (access, portability, erasure, right to object, etc.) will generally provide end-users with the most effective level of control over their data. Confidentiality is guaranteed through **technical and organisational measures** designed to preserve and maintain the integrity, authenticity and selective disclosure of communications, including measures such as two-step authentication, pseudonymisation/key-coding, anonymisation, encryption, rotating hashing, and storage policies.

Recommendation: We strongly recommend introducing well-established legal bases to process communication metadata and content data, including (i) processing necessary for entering into or for the performance of a **contract** and (ii) processing based on the **legitimate interest** and which does not override the interests or the fundamental rights and freedoms of the end-user(s). The proposal should also allow for **further processing for compatible purposes** under the conditions laid out in the GDPR. Furthermore, **multiple consents from all parties to a communication should be removed** under Article 6(3)(b). Lastly, **consent-withdrawal notification every 6 months should be removed.**

>> see suggestions for amendments to Articles 6 and 9(3).

4. Confidentiality restriction for law enforcement purposes: safeguards & legal certainty

We are concerned that the proposal extends the confidentiality exemptions of the current e-Privacy rules well beyond traditional law enforcement purposes, to any "other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security"[10]. We believe that any restrictions to the rights found in Articles 5 to 8 should be subject to strict, detailed and clear proportionality and necessity tests to differentiate exigent cases from ordinary circumstances. In addition, any restriction should be subject a clear set of safeguards and remedies enshrined in law, consistent with CJEU case-law.

Furthermore, Article 11(2) broadly prescribes all ECS providers subject to the E-Privacy regulation to establish internal procedures to respond to requests from national authorities governed by national laws. This provision would constitute a disproportionate burden on many services where communications have little to no interest for law enforcement or regulatory authorities (e.g. potentially any platform that provide ancillary communications services and IoT services built smart devices).

We are also concerned that Article 11(2) does not lay down any safeguards or limitations which authorities should observe on a case-by-case basis. any interference with the right to confidentiality of communications should be clearly and only defined by law. Such law should enshrine adequate procedural and substantial safeguards to ensure that the scope of the requests be limited to what is strictly necessary, and that they are duly justified and approved by a judicial or independent authority.

[10] Article 11(1) of the proposal read together with Article 23(1)(e) of GDPR

Most importantly, Article 11(2) preempts and risks conflicting with the upcoming proposal on law enforcement access to e-evidence. The extent to which electronic communications service providers should facilitate data access for law enforcement purposes and the necessary safeguards should be comprehensively addressed in a separate legislation, i.e. the upcoming proposal on law enforcement access to e-evidence. At this stage, we recommend that Article 11(2) should only compel ECS providers to respond to law enforcement requests in accordance with the legal requirements of the Member State where the provider has its main establishment.

Recommendation: The grounds for restriction to the right to confidentiality of communications should be limited to what is strictly necessary, appropriate and proportionate within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, as referred to in Article 23(1)(a)-(d) of the General Data Protection Regulation.

Pending the publication and review of the upcoming proposal on law enforcement authorities access to e-evidence, Article 11(2) should clarify that ECS providers may only respond to disclosure requests in accordance with the legal requirements of the Member State where the provider has its main establishment.

>> See suggestions for amendments to Article 11 and Recital 26

Fostering a protective, fair and rich online ecosystem

CCIA supports the stated objective of the proposal to reform of the current "cookie" rule and do away with multiple and iterative consent requests. Unfortunately, we regret to see that the **proposed Articles 8, 9 and 10 not only exacerbate the existing problems** of the current framework, **but create new ones** by adding a new consent "mechanism" which would be inconsistent with the consent standard established in the GDPR. Furthermore, the proposal **undermines the principle of technology neutrality** and **risks undermining the current digital ecosystem, without increasing end-users' privacy protection.**

CCIA recommends fixing these problems by:

- Adopting a context- and risk-based approach on the collection and processing of personal data from the end-user's device, in line with the GDPR. The EPR should leave sufficient flexibility and additional legal grounds for service providers to choose and implement the most privacy-friendly measures for a given purpose of processing;
- Removing inconsistencies with regard to consent;
- Encouraging market-led, technology neutral solutions for software privacy settings
- Allowing content access to be conditional on cookie acceptance

1. Fostering privacy-enhancing measures through additional legal grounds for cookie-based data processing

We support the end of cookie banners which are widely perceived to hamper end user experience. However, the proposed Article 8 does very little to help achieve this goal since it maintains consent as the main legal ground for the placing of cookie technologies and the collection and processing of information about end-users' devices, regardless of the purpose of processing and the privacy-mitigating measures which have been put in place.

We would like to recall that, in the context of the GDPR, the Article 29 Working Party suggests to use all legal bases and rely on consent when it is the most appropriate. Indeed, the best way to avoid "consent fatigue" is to ensure that it is relied upon when it is most meaningful. There are a range of other ways to ensure transparency and control for the user, and the other legal grounds of the GDPR also entail the adduction of a range of different technical and organisational safeguards.

We believe that **legitimate interest and the built-in safeguards therein**, coupled with the right to object under the GDPR, **can provide an adequate level of privacy protection while leaving breathing room for some value-generating processing**, including processing for advertising purposes. We recall that online advertising funds a a myriad of new and well-established services which are offered to citizens and private organisations either for free, or at reduced rate.

The use of legitimate interest as a legal ground for processing requires careful considerations from the service provider (or "data controller") on the envisaged processing. Among others, services providers must clearly identify the scale and type of the data and the frequency of the expected processing, identify specific interests and purposes for the processing, anticipate the expectations of the end-user, map out the implications for the end-users that the processing may entail, and calibrate and apply appropriate technical and organisational measures to mitigate potential risks to the fundamental rights and interests of end-users (or "data subject"), e.g. pseudonymization.

As a result, the extensive evaluation of the envisaged processing that is required to use legitimate interest as legal basis shifts the burden away from the end-user to the service provider. Introducing further flexibility does not preclude the use of consent. It just allows for finding the right legal basis that is most appropriate for a given processing.

Recommendation: We encourage lawmakers to incentivise the use of privacy-enhancing technologies and enshrine the **legitimate interest as a lawful ground** to process personal information via cookies and other similar techniques for the purpose of advertising. This would still require the provider to ensure the **respect of interest and fundamental rights and freedoms of the end-user through the balancing test required in the GDPR, and that the processing reflects the users' reasonable expectations.**

>> See suggestions for amendment to Article 8 and Recitals 20, 21.

2. Ensuring a consistent principle-based approach to consent

Article 9(2) of the proposal effectively creates a **new consent standard** through software setting configuration which would be **inconsistent with the consent regime established by the GDPR** (and its predecessor, Directive 95/46/EC).

A one-size-fits-all consent mechanism, such as through software setting configuration as foreseen in Article 9(2), is unlikely to be deemed valid. As explained in existing and new guidance from the Article 29 Working Party[11], consent can only be valid if it meets several criteria, including if it is sufficiently granular and targeted to specific

[11] See Article 29 Working Party opinions WP187 and WP208, and guidelines WP259

processing operations, and if the data subject / end-user is adequately "informed" about the purpose of a given processing operation.

Furthermore, and in the Commission's own admission, this provision provides **no added-value from the end-user's perspective and would not change the status quo when it comes to cookie banners**. As the Commission rightly points out in its explanatory memorandum, "centralising consent [as per the proposed Article 9(2)] does not deprive website operators from the possibility to obtain consent by means of individual requests to end-users [...]."[12]

We believe that regulation has an important role to play in defining consent at a principle level to ensure a future-proof framework for service providers across the digital value chain to obtain valid consent. However, lawmakers should avoid imposing specific mechanisms which may become obsolete as technology evolves.

Recommendation: The consent mechanism in the EPR should be fully aligned and consistent with the legal standard set forth in the GDPR. We recommend removing Article 9(2).

>> See suggestions for amendment to Article 9(2) and Recital 22.

3. Encourage market-led, technology neutral software privacy settings

CCIA is concerned with the proposed provision to impose an obligation on all "software permitting electronic communications" to offer end-users to accept or reject third-party cookies. If adopted, this provision would breach the principle of technology neutrality and fundamentally alter today's digital architecture.

We would like to underline that Article 10 of the proposal mandates developers and distributors of **all kinds of software providing access to the Internet** - ranging from operating systems, VoIP applications and other apps, connected hardware drivers to screenless IoT software interfaces - **to act as gatekeepers of the Internet by using the logic of one particular technology, namely browsers.**

This provision also **favours a narrow set of "first-party" cookies**, developed in-house, over cookies developed and deployed by third parties, **regardless of the purpose of processing** (be they security cookies, audience measurement cookies, online shopping session cookies, permanent login cookies, etc.), **the "risks" or lack thereof which different third-party cookie processing may entail,** and **regardless of whether cookies are deployed and ran on behalf of a website owner** (as "controller") **by a third-party** (as "processor"). Furthermore, a domain owned by the same company may serve cookies to its other domains, to keep pseudonymised data separate, for example. These would be picked up as third-party cookies despite both domains belonging to the same company. The absence of consideration to context, purpose, and privacy risks depart from the approach of the GDPR.

As explained earlier, we believe that regulation has an important role to play in setting out the broad conditions for valid consent so as to ensure a future-proof framework for all service providers across the digital value chain. However, lawmakers should refrain from imposing specific mechanisms which may become obsolete as technology evolves.

[12] See page 8 of the explanatory memorandum of the proposal.

Erecting browsers as gatekeepers for “third party” cookies could also severely impact end-users’ daily browsing experience, and prevent companies from creating and maintaining a direct and trusted relationship with their customers / users, and conveying the benefits of all third party cookies they may use - from maintaining session IDs to accessing free, advertisement-funded content and services.

CCIA Europe supports meaningful browser settings which end-users can understand. Today, competing browsers already offer privacy settings, making the intention to regulate browsers in ePrivacy redundant and unnecessary.

Recommendation: Instead of trying to codify certain browsers settings in law and impose them on a wide range of software that provides access to the Internet, we suggest to delete Article 10 and the corresponding recitals.

>> See suggestions for amendment to Article 10 and Recitals 23, 24.

4. Access to content and services should be made conditional on cookie acceptance

While the end-user should be free to decide whether to consent to the collection of data from cookies, (s)he should still bear the consequences of his or her choice. To prohibit cookie walls or compel service providers to offer alternative solutions to access content or services would disproportionately encroach upon the principle of contractual freedom and the freedom to conduct a business, let alone question the basic economics of a “transaction”.

By way of analogy, it would be unthinkable in the physical world for anyone to access a service or own a good without purchasing them. Nor would it be reasonable to mandate the service provider or the seller of a good to offer alternative forms of "payment". We see no reasons why it should be any different in the digital realm.

We draw lawmakers’ attention to the fact that many online service providers, particularly smaller players, rely on third party cookie-based advertising to generate revenue and maintain and improve their services. The prohibition of cookie walls and/or the obligation to provide alternative solutions would therefore have severe detrimental effects upon them.

Recommendation: In case the end-user refuses to consent to the processing of his or her data, the ePrivacy Regulation should **explicitly leave the choice to service providers to either refuse to grant access to the service / content, in line with the existing regime** (see Recital 25 the E-Privacy Directive).

>> See amendments to Article 9(1a) NEW.

***

For further information, please contact Alexandre Roure at aroure@ccianet.org.