BEUC The European Consumer Organisation

The Consumer Voice in Europe

BEUC RECOMMENDATIONS FOR THE TRILOGUE NEGOTIATIONS ON THE PROPOSED E-PRIVACY REGULATION

Contact: David Martin – digital@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2021-106 - 17/11/2021

Why it matters to consumers

Consumers need a robust legal framework that protects their fundamental rights to privacy and data protection to ensure they can benefit from the digital economy and trust online services. The e-Privacy rules specifically protect the confidentiality of communications and ensure the protection of consumers' devices (e.g. smartphones and computers) against unwanted intrusions and online tracking. These rules are essential to guarantee that consumers' online activities cannot be monitored without their permission.

Summary

BEUC reiterates the urgent need to better protect consumers' privacy online and calls for a swift agreement on the proposal for an ePrivacy Regulation (ePR). The agreement must ensure that the ePR strengthens the level of protection granted under the current ePrivacy Directive (ePD) and the General Data Protection Regulation (GDPR). Any measure that weakens the existing legal framework should be seen as crossing a red line, particularly if it relates to the legal basis for processing communications data and the protection of terminal equipment.

BEUC considers that the European Parliament's position and the recommendations put forward by the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) provide a good basis for an agreement. In contrast, the Council's position raises concerns as it would weaken the level of protection of consumers' privacy and deviate from the main objective of the proposal: increasing the protection of people's private life and reinforcing trust and security in the digital world.

The ePR must provide consumers with improved, stronger, protections to complement the rules of the GDPR and ensure that they can fully enjoy the benefits of the digital world without being forced to give up their privacy.

In particular, we call on the co-legislators to ensure the following in the final text of the regulation:

- **Article 6 should not include the possibility of carrying out further processing for "compatible purposes"**. The EU must strongly protect confidentiality of communications. It should not be possible to process communications data, in particular metadata, under broad legal grounds and for unspecified purposes. Processing electronic communications data without consumers' consent must be limited to purposes related to the transmission of the communication or technical purposes such as ensuring the security of the services.

- **Article 8 not include a legal ground to access or process any information from consumers' terminal equipment for "compatible purposes"**. The possibilities of accessing consumers' terminal equipment without their consent must be strictly limited and precisely defined. It should not be possible to access terminal equipment under broad legal grounds and for unspecified purposes.

- **Article 8 should include a clear ban on "tracking walls''**. Consumers' behaviour and activities should not be monitored without their consent. They should be able to have access to digital services without being forced to accept unnecessary invasions of their privacy.

- **Article 10** should be maintained and include a clear obligation to ensure that the settings of software and hardware are set to the most privacy-protecting options by default **('Privacy by Default'**). If Article 10 is not included in the final text of the Regulation, this obligation should be integrated as a new element in Article 8.

BEUC Recommendations for the trilogue negotiations on the proposed ePrivacy Regulation

1. Background

In January 2017, the European Commission put forward a proposal for a Regulation on Privacy and Electronic Communications ("ePrivacy Regulation", "ePR")[1]. This regulation, which would replace the existing e-Privacy Directive ("ePD"), is a crucial instrument to protect consumer's privacy in the Digital Age. It complements the General Data Protection Regulation ("GDPR") and helps create a comprehensive legal framework for the protection of consumers' privacy in the digital environment, a key element to increase consumer trust in this area.

In October 2017, the European Parliament adopted a strong and consumer-friendly position as its mandate for trilogue negotiations.[2] After long deliberations, the Council adopted its mandate for negotiations in February 2021.[3] The position of Member States raises several concerns, as it would weaken the protection of consumers' privacy, notably in relation to the confidentiality of their communication and the protection of their terminal equipment.

In May 2021, Parliament and the Council started trilogue negotiations to reach a final agreement over the proposed regulation[4].

2. Recommendations

First, BEUC would like to reiterate the urgent need to better protect consumers' privacy online. We call on the co-legislators to reach a swift agreement on the ePrivacy Regulation proposal. They must ensure that the ePR strengthens the level of protection granted under the current ePrivacy Directive and the GDPR. Any measure that weakens the existing legal framework should be seen as crossing a red line, particularly on issues related to the legal basis for processing communications data and the protection of terminal equipment.

We consider that the European Parliament's position and the recommendations put forward by the European Data Protection Supervisor (EDPS)[5] and the European Data Protection

[1] https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation
[2] https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html
[3] https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf
[4] https://www.patrick-breyer.de/en/eprivacy-regulation-trilogue-negotiations-start-today/
[5] https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

Board (EDPB)[6] provide a good basis for an agreement. The ePR must provide consumers with improved, stronger, protections to complement the rules of the GDPR and ensure that they can fully enjoy the benefits of the digital world without being forced to give up their privacy. Below we outline key points to ensure that the ePR achieves this objective.

Electronic communications data should only be processed for concrete, strictly defined purposes (Article 6)

While the European Commission proposal and the Parliament's position already foresee an expansion of the possibilities to process communications data beyond the current ePrivacy Directive, the Council's position goes too far by enabling the further processing of electronic communication metadata without the consent of consumers.

In particular, the Council would allow further processing of any pseudonymous communication metadata for a different purpose if the data processing is 'compatible' with the purposes for which the data was originally collected.

Firstly, pseudonymous data is still a form of personal data and must be fully protected as such, as it always allows for some form of re-identification. Secondly, metadata can reveal very sensitive information such as who you call, how often, how long a conversation lasts, your location, etc. It can sometimes say more about individuals than the content of their communications. The European Court of Justice has also explicitly stated in several rulings that very sensitive and personal information can be disclosed through metadata, and that it should therefore be strongly protected.[7]

***Article 6 should not include the possibility to carry out further processing of electronic communications data for "compatible purposes"**, in line with the original Commission proposal and the European Parliament position. The EU must protect the confidentiality of communications. It should not be possible to process communications data, be it content or metadata, under broad legal grounds and for unspecified purposes. Processing electronic communications data without consumers' consent must be limited to purposes related to the transmission of the communication or technical purposes such as ensuring the security of the services.*

Consumers must be strongly protected against intrusions into their terminal equipment and online tracking (Article 8)

Access to terminal equipment

Corporate surveillance is one the main problems that consumers face in the digital world. Extensive tracking and profiling techniques, deployed often (but not only) for targeted advertising purposes, can be (ab)used to discriminate against categories of consumers and manipulate their behaviour. This can have substantive negative implications for consumers and seriously undermine their fundamental rights and freedoms, as shown in recent research by BEUC's Norwegian Member, the Norwegian Consumer Council (NCC).[8]

The Commission proposal and the Parliament position already extend the possibility to access terminal equipment without user consent beyond what is currently permitted under the ePrivacy Directive. We support some extensions, notably those related to first party audience measurement and analytics, provided that there are sufficient safeguards. However, the Council also goes too far on this point by allowing processing for "compatible

[6] https://edpb.europa.eu/system/files/2021-03/edpb_statement_032021_eprivacy_regulation_en_0.pdf
[7] E.g. see Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger
[8] "Out of Control – How consumers are exploited by the online advertising industry", NCC, 2020

purposes" of information stored on users' terminal equipment, without their consent. This exception is vague, unclear and unacceptable from our perspective. Terminal equipment contains a trove of consumers' most personal information. Devices such as smartphones are at the centre of consumers' digital activities. They can be used to track consumers' every move[9], in the online and physical worlds. Access to such equipment should therefore be strictly regulated.

***Article 8 should not include a legal ground to access or process any information from consumers' terminal equipment for "compatible purposes"**, in line with the European Commission proposal and the Parliament position. The possibilities to access consumers terminal equipment without their consent must be strictly limited and precisely defined. It should not be possible to access terminal equipment under broad legal grounds and for unspecified purposes.*

Tracking walls

Consumers are still often faced with 'take it or leave it' situations, where providers make access to services and functionalities conditional on getting the consumer's consent to store
information, or gain access to information already stored, in the consumer's terminal equipment. These 'tracking walls' are often used with the aim of forcing consumers to accept being tracked and profiled for targeted advertising purposes.

BEUC recognises the importance that advertising has for the funding of internet services and online content, as well as the legitimacy of ad-funded business models. However, we are strongly concerned about the predominant online advertising business model which operates at the expense of consumers' privacy, based on 24/7 surveillance and monetisation of consumers' every move by a myriad of entities (advertisers, publishers, advertising networks, ad-exchange platforms, data brokers, etc.). This specific type of targeted advertising, referred to as 'surveillance-based advertising', is harmful to consumers.[10]

Calls to take decisive action against online tracking and surveillance based advertising are steadily growing.[11],[12] The ePrivacy Regulation is a clear opportunity to do something to create a fairer and more privacy-friendly digital environment. 'Tracking walls' should be explicitly prohibited. Users must not be denied access to a service if they refuse to accept to be tracked for purposes that are not strictly necessary. This is compatible with services being funded through advertising. Advertising does not necessarily have to be privacy-invasive. Other forms of advertising technologies exist, which are economically viable[13] and do not depend on spying on consumers.

Consumers' behaviour and activities should not be monitored without their consent, and they should be able to have access to digital services without being forced to accept unnecessary invasions of their privacy.

The Commission proposal did not include any specific measures against tracking walls, but the European Parliament's position rightly introduced a ban.[14] On the contrary, the amendments contained in the Council' position would legitimise the use of such walls.

---

[9] "Every Step You Take: How Deceptive Design Lets Google Track Users 24/7", NCC, 2018
[10] "Time to ban surveillance based advertising", NCC, 2021
[11] E.g. see Tracking Free Ads Coalition
[12] 'International coalition calls for action against surveillance-based advertising', NCC, 2022
[13] https://techcrunch.com/2020/07/24/data-from-dutch-public-broadcaster-shows-the-value-of-ditching-creepy-ads/
[14] See EP Amendment 92 – Article 8 – paragraph 1a (new)

***Article 8 should include a clear ban on "tracking walls"**, in line with the European Parliament's position. No entity should monitor consumers' behaviour and activities without their consent. It must be made very clear that consumers can access digital services without being forced to accept unnecessary invasions of their privacy.*

Privacy friendly settings should be the default

The Flash Eurobarometer on ePrivacy[15] clearly showed that consumers want privacy-friendly default settings.[16] This is important because many consumers do not have the necessary technical skills to understand and configure their devices and apps to protect their privacy. In particular, the Flash Eurobarometer on ePrivacy shows that older people, and people with low levels of education are less likely to change the privacy settings of their software.[17] Privacy-friendly default settings are therefore particularly important to protect these vulnerable consumer groups.

Article 10 of the European Commission proposal did not include a "privacy by default" obligation but the European Parliament rightly introduced such an obligation in its position. It also reinforced the information obligations in the original proposal and the binding nature of the choices expressed by the user through their choice of settings.[18]

On the contrary, the Council deleted Article 10 completely and underlined that, while it should be possible for users to express consent via browser settings, any consent directly expressed to a particular service should override the settings immediately. This approach would be problematic. First, because of the importance of providing privacy protection by default. Second, because it would disadvantage privacy-friendly browsers that do provide such protection by default. Third, because it would not help reduce consumers' repeated exposure to consent banners, nor protect them against the manipulative practices deployed in such banners to nudge consumers to give consent to be tracked and profiled.

***Article 10 of the proposal should not be deleted. It should include a clear obligation to ensure that software settings are set to the most privacy protecting options by default ('Privacy by Default')**, in line with the European Parliament's position. Specific 'Privacy by default' obligations are an essential layer of protective measures for consumers and represent one of the added values of the ePrivacy Regulation. If, in the end, Article 10 is not included in the text of the Regulation this obligation should be integrated as a new element in Article 8.[19]*

For more information on BEUC's position on the proposed ePrivacy Regulation:

- BEUC Factsheet on ePrivacy
- BEUC position paper on the ePrivacy Regulation proposal
- BEUC Factsheet 'Consumers caught in a tracking web'

[15] Flash Eurobarometer 443, December 2016
[16] 89% of respondents agreed that the default setting of their browser should stop their information from being shared
[17] See page 37, Flash Eurobarometer 443.
[18] See EP Amendments 106-118 to Article 10.
[19] See suggested amendments from AccessNow, EDRi and NOYB, Article 8.1c, page 106

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).