The Consumer Voice in Europe

# CONSULTATION ON THE REVIEW OF THE E-PRIVACY DIRECTIVE

## SUMMARY OF BEUC RESPONSE

**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 • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2016-073 - 04/08/2016

# Why it matters to consumers

The digital revolution has brought enormous benefits to consumers, but it has also created significant challenges for the protection of their privacy. A robust legal framework that protects consumers' fundamental rights to privacy and data protection is necessary to ensure that they can safely benefit from the Digital Economy and trust online services. The upcoming General Data Protection Regulation (GDPR) represents a significant step forward. Now it is necessary to update the e-Privacy Directive to adapt it to technological developments, such as the raise of Over-the-top communication platforms ("OTTs"), and to ensure consistency in the legal framework. It is essential to protect the confidentiality of communications and guarantee a high level of consumer privacy protection across all services.

## SUMMARY OF BEUC RESPONSE TO THE EC PUBLIC CONSULTATION

### Effectiveness of the e-Privacy Directive

The e-Privacy Directive is an important instrument to protect privacy and the confidentiality of communications. Its specific privacy rules for the electronic communications sector have a clear added value. However, it has not been able to achieve full protection, as for example persisting problems around online tracking and profiling have not been resolved.

The Directive has been helpful in trying to ensure a high level of protection within electronic communications services but the lack of consistency in terms of its implementation and enforcement have diminished its impact and created fragmentation.

Moreover, the emergence of over-the-top ("OTTs") online communication services (like Voice over IP or instant messaging applications) and other means of communication via information society services, has exposed limitations and gaps in the current rules. These new services are massively used by European consumers but they currently fall outside the scope of the Directive. This means for example that a consumer sending a message over an OTT service like WhatsApp does not enjoy the same legal protection as when sending an SMS over a traditional telecoms operator. Consumers are not aware and do not understand these differences in protection.

Also, the obligation for the user to consent for the use of website 'cookies' has not yielded the desired result. Users are receiving warning messages in almost every website but the consent request is very often just an 'illusion', a 'take or leave it' choice where there is no option but to agree. Moreover, cookies are often placed in the users' equipment even before they have given their consent.

Confusion might have been created as well by the fact that the Directive has been transposed differently by the member states and different authorities are competent for its enforcement. A consumer might logically think that for privacy related issues it would be the data protection authority that is responsible, not the telecoms regulatory authority for example, and this is not always the case.

## Relevance and efficiency of the e-Privacy Directive

The e-Privacy Directive is still relevant and necessary. The General Data Protection Regulation (GDPR) formulates the general framework applicable to the processing and use of personal data in the EU. However, due to the risks and specificities of the electronic communications sector and the online environment, sector specific rules are justified and necessary, not only for traditional electronic communication services but also for OTT communication services and, more broadly, information society services in general.

The e-Privacy Directive is the only legal instrument that crystallises Article 7 of the European Charter of Fundamental Rights (on the protection of private life and communication) into secondary EU law and specifically protects the confidentiality of communications.

The e-Privacy directive, as transposed at national level, has somewhat helped to create a safer environment for users' privacy. Nevertheless, public surveys, such as the latest Data Protection Eurobarometer, show that a majority of citizens do not trust landline or mobile phone companies and internet service providers, or online businesses. A recent study published by the Open Rights Group in the UK also illustrates how phone companies are exploiting their customers' data. The rise of OTT services has also exposed the limitations of the existing rules.

Therefore, more needs to be done to guarantee the full respect of consumers' fundamental rights to privacy and data protection. Strengthened e-Privacy rules are necessary. It is clear that in the absence of the e-Privacy rules, issues of concern such as data mining and tracking/profiling of users could grow even larger in scale and the confidentiality of our communications would be unprotected at EU level.

## Review of the e-Privacy Directive

*Scope and choice of instrument*

The scope of the Directive should be broadened so that OTTs offer the same level of protection when they provide communications services such as Voice over IP and instant messaging. Where appropriate, the scope should go beyond OTT communication services and cover all information society services in general, complementing the rules of GDPR and particularising them to ensure a high level of data protection and privacy in the online environment, in line with articles 7 and 8 of the European Charter of Fundamental Rights.

The e-Privacy obligations should also apply to non-commercial Wi-Fi internet access which is available to the public (e.g. Wi-Fi available to the customers in a restaurant, an airport or a shopping centre).

In terms of the legal instrument, a Regulation would help ensure consistency with the GDPR and guarantee a uniform high level of protection in all Member States.

*Security and confidentiality of communications*

It is essential to ensure the protection of the confidentiality of communications and that 'privacy by design' and 'privacy by default' become fundamental guiding principles in the online environment. The legislation should also ensure the right of individuals to secure their communications.

Consumers' daily use of digital technology continues to increase and connected devices are set to become ubiquitous in the near future. Users should always have the right to secure their networks, equipment and communications with the best available techniques. On the other hand, providers of electronic communication services should be obliged to secure all communications by using the best available techniques to ensure security and confidentiality.

*Consent requirement to access users' devices and tracking of users*

The obligation under Article 5(3) of the Directive to have users' consent in order to access their devices must be maintained. Moreover, information service providers should not have the right to prevent access to their non-subscription based services if users refuse the storing of identifiers that are not necessary to provide the service in their terminal equipment.

The 2015 Data Protection Eurobarometer shows that a majority of Europeans is uncomfortable with internet companies using information about their online activity to tailor advertisements. Consumers should have the possibility to use online services without being under constant commercial surveillance. This is not incompatible with services being funded through advertising, as advertising does not necessarily have to be targeted and/or privacy invasive. There are alternatives to behavioural advertising, e.g. context-based advertising or advertising based on information about interests actively provided by the user. A report published by the Norwegian Data Protection Authority in January 2016 shows that a large majority of users (73%) would prefer random advertising to targeted advertising (27%).

On the other hand, this does not mean that every website should be forced to offer a paying service alternative. Such an obligation could foster social/economic discrimination (i.e. the rich, who can pay to protect their privacy, and the poor, who cannot) which would run against the universal nature of the fundamental rights to privacy and data protection. Forcing websites to offer a paid subscription service could also interfere with the development of new innovative business models which might be advantageous to consumers.

The use by service providers of tools to disable or circumvent 'anti-tracking tools' used by consumers should be prohibited unless the consumer has given prior explicit consent.

The e-Privacy instrument should complement the GDPR provisions on profiling. Future-proof rules are needed to cover any type of tracking mechanisms that could be eventually developed. This concerns identifiers placed in users' devices but also other mechanisms (e.g. device fingerprinting and web beacons). There are no tools to easily stop tracking via these mechanisms. Cross-device tracking is also problematic and should be addressed.

That being said, it's also important to avoid constant 'consent requests' which could disturb users' online experience and lead them to 'routinely' accept such requests. An exception for innocuous technical mechanisms used for the correct functioning of a service should be foreseen. This exception should only apply to mechanisms that pose no privacy risks and strict purpose limitation must be ensured. Exceptionally intrusive tracking methods (e.g. 'super cookies') should be forbidden. The lifespan of cookies should be limited in connection to their purpose.

It is also essential that the e-Privacy rules on consent remain consistent with the GDPR.

*Traffic and location data*

The consent requirement for the processing of traffic and location data should be maintained and the exemptions to this rule should not be broadened.

Traffic and location data can provide a very detailed picture of an individual's habits, acquaintances and daily routine. A study carried out by Stanford University researchers in the US showed that it is possible to guess individuals' names, addresses and the names and numbers of their partners just by knowing whom they had called and texted. Not only that, the researchers were also able to identify specific individuals who suffered from serious health conditions.

GPS location data and Wi-Fi network location data used by information society services in mobile devices is even more accurate than traffic and location data collected by telecoms providers and should therefore be covered in the future e-Privacy instrument. Moreover, in no case it should be allowed to process traffic and location data for direct marketing purposes on the basis of Article 6.1 (f) of the GDPR.

Traffic and location data should only be processed with the consent of the user and, like any other personal data, should be reduced to the minimum necessary for the purpose for which they are collected and used, and deleted as soon as they are no longer needed. Traffic and location data should be reduced to the least-granular that is needed for the purpose for which they were collected and only used for legitimate and compatible purposes. We would also like to stress that the anonymization of location data is also challenging, as combined location data might still lead to identification (see Opinion 13/2011 of the Article 29 Working Party).

*Non-itemised bills, call line identification, automatic call forwarding and subscribers directory*

All these provisions should be maintained. Like metadata, itemised bills can be very revealing. Also, consumers need to continue to be able to control whether their personal data is made publicly available or not. They should also be able to protect their anonymity when calling and be able to block automatic call forwarding by a third party to their terminals.

*Unsolicited commercial communications*

Marketing messages sent through social media should be subject to the same opt-in obligation that applies to email.

Due to our members' perception that in a few countries the opt-out system for telemarketing calls seems to be working reasonably well, we consider that introducing a harmonised 'opt-in' obligation for this is not required at this stage. However, the current provision allowing Member States to decide between an 'opt-in' or 'opt-out' system should be reinforced by requiring that those Member States choosing to use an 'opt-out' system ensure that there are effective safeguards to guarantee compliance and strong enforcement.

*Competent enforcement authority*

In order to ensure consistency and benefit from the enforcement system developed under the GDPR, Data Protection Authorities (DPAs) should have full competence over the enforcement of the future e-Privacy instrument. DPAs are the best equipped, both in terms of expertise and legal powers, to deal with privacy related issues.

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