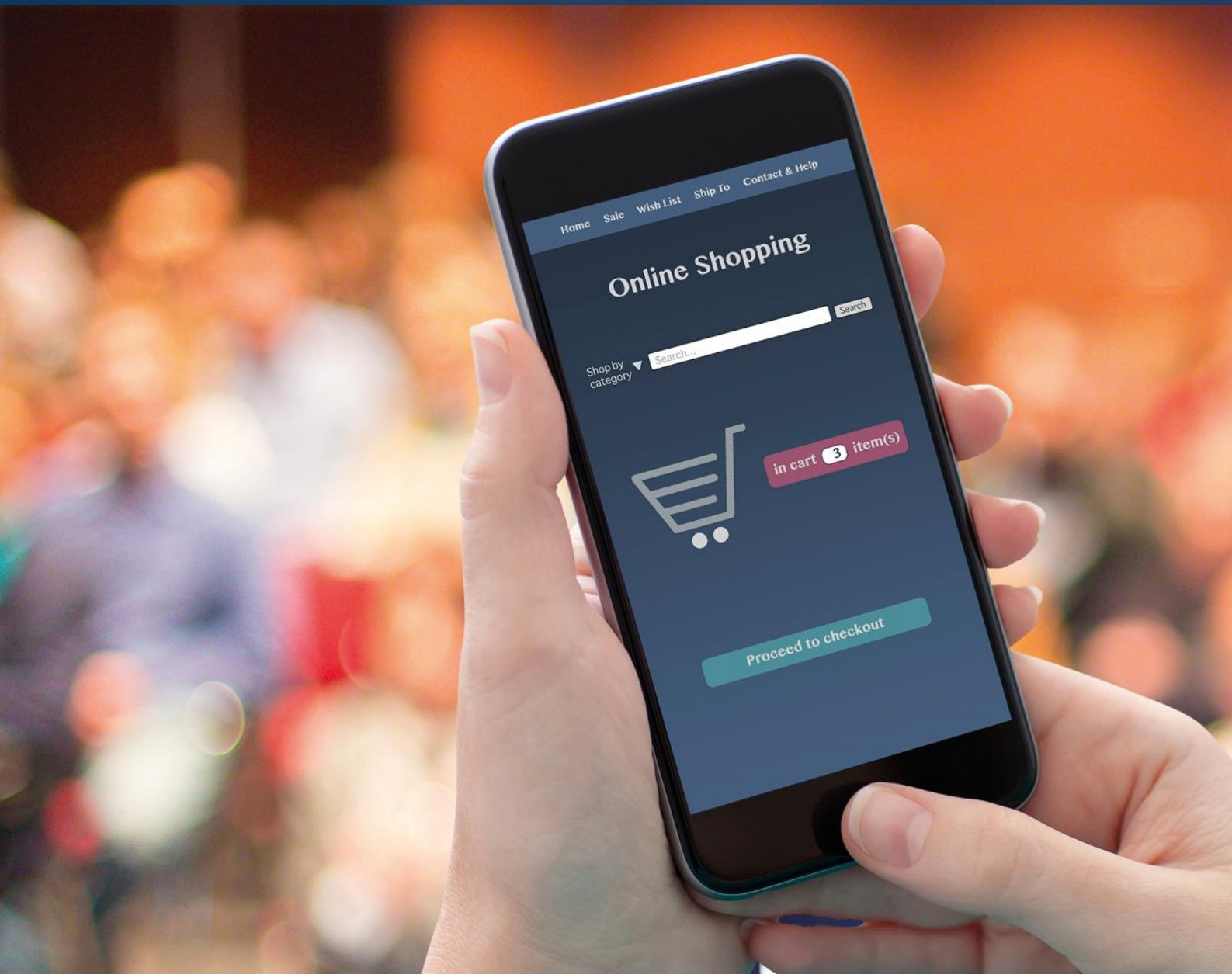
ECOMMERCE EUROPE POSITION PAPER

Policy recommendations for a better Regulation on Privacy and Electronic Communications

July 2017



ECOMMERCE EUROPE

INTRODUCTION

In January 2017, the European Commission proposed a new legislation to ensure stronger privacy in electronic communications, the Proposal for a Regulation on Privacy and Electronic Communications[1]. Overall, Ecommerce Europe has always supported the idea of modernizing the current ePrivacy Directive in order to make the ePrivacy legal framework fit for the future of online retail. Ecommerce Europe also welcomes the choice for a regulation as legislative tool, because it will achieve a higher degree of harmonization compared to a directive and it will reduce the risk of "gold plating" from Member States. Nevertheless, Ecommerce Europe is concerned about some provisions included in the draft ePrivacy Regulation, which are further explained in this position paper. Ecommerce Europe developed specific recommendations for EU policymakers, based on the text of the European Commission's Proposal and Draft Report of MEP Marju Lauristin (EP, LIBE)

RECOMMENDATIONS FOR EU POLICYMAKERS

Exclude the processing of personal data from the scope of the Regulation

This Regulation applies to electronic communications services and the processing of data and content carried out in connection with the provision and the use of electronic communications services. It mainly aims to regulate:

- confidentiality of electronic communication;
- processing of personal and other data in the course of electronic communications;
- access to information related to the terminal equipment of end-users and placing of information on the end-users terminal equipment;
- unsolicited commercial electronic communications

Ecommerce Europe sees a clear need to upgrade and cover the existing rules on confidentiality of electronic communications, on access to the terminal equipment of the end-user and the information on it and on unsolicited commercial communications. However, Ecommerce Europe does not see any need to introduce new rules for the processing of data or personal data in the course of electronic communications, as this subject is sufficiently covered by the provisions of the well-balanced GDPR, which will be applicable as of 25 May 2018.

In the view of Ecommerce Europe, there is absolutely no evidence for a need for special rules on data processing and privacy in electronic communications diverging from the GDPR and giving either less or more protection to data subjects than the level already provided by the GDPR. Such diverging rules are not only obsolete but they also make the legal framework on the processing of personal data unnecessarily complex. That is why Ecommerce Europe strongly advocates to refrain from introducing

[1] COM(2017) 10 final - 2017/0003 (COD)

any new rules on the processing of personal data in the course of electronic communications and leave this subject entirely to the GDPR. This also means that the new ePrivacy Regulation should carefully refrain from any reference in the recitals to the protection of personal data as a goal or basis for the proposed law (as in recitals 4, 5 and 7) and should also refrain from regulating the processing of personal data in the course of electronic communications. In this view, Ecommerce Europe strongly suggests deleting from the draft ePrivacy Regulation the last part of Sections 1 and 2 of Article 1 "and on the protection of natural persons with regard to the processing of personal data" and also delete Section 3 of this Article and Section 5 of Article 3.

Instead of focusing on the processing of personal data and privacy aspects which are sufficiently covered by the GDPR also for electronic communications, the Regulation should focus on the right on confidentiality of electronic communications. This makes perfect sense given the fact that the main issues of the ePrivacy framework (confidentiality of electronic communication content and metadata, respect for the private sphere of the terminal equipment of the end-user and respect for a natural persons' electronic mailbox) are based on the fundamental right of respect for everyone's private and family life, home and communications, as laid down in Article 7 of the Charter of Fundamental Rights of the European Union (the Charter) and not on the fundamental right to the protection of personal data, as laid down in Article 8 of the Charter and Article 16 of the Treaty on the functioning of the European Union.

Restrictive rules on permitted processing of confidential electronic communications should only be applicable on the content of electronic communications

Ecommerce Europe strongly agrees that the content of electronic communication, the communication as such - as defined in Article 4 of the Proposal - shall be confidential. Ecommerce Europe supports any regulation that prohibits interference with this electronic communication, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of the content data, by persons other than the end-users, except when permitted by this Regulation. Ecommerce Europe also agrees that electronic communication metadata shall, when relevant, be confidential. However, electronic communications metadata do not share the characteristics of electronic communication content. In the view of Ecommerce Europe, metadata do not reveal any information on the content of electronic conversations and should therefore not be subject to the strict regime on permitted processing of confidential content of Article 5 Section 3, nor to the restricted regime of Article 5, Section 2. According to Ecommerce Europe, processing of electronic metadata should be allowed on the same grounds as provided for by Article 6 of the GDPR and, thus, also cover billing (performance of the contract).

In particular, the proposed ePrivacy Regulation provides for a number of provisions governing the conditions under which an enterprise can send electronic commercial communications to an individual. There should be a clear distinction between the GDPR, which deals with the collection and processing of personal data for direct marketing purposes (privacy and personal data protection), and the future

ePrivacy Regulation, which specifies the conditions for sending electronic commercial communications to an individual (respect for privacy). Moreover, it is important to stress that consent for cookies is indeed based on the same principle as consent for processing personal data. Nevertheless, the purpose is different: on the one hand, it is consent for placing a cookie on the terminal equipment of the end-user and, on the other hand, it is consent for processing personal data. Understanding this distinction is essential to ensure that the new ePrivacy Law will not duplicate the existing rules of the GDPR, but will focus only on the conditions for sending and receiving commercial electronic communications.

Permitted processing of electronic communications content and metadata: for content, restrict Article 6 to Section 3 and, for metadata, align with Article 6 GDPR

For permitted processing of electronic communications content, Ecommerce Europe can agree with the proposed wording of Sections 3 and 1 of Article 6 of the ePrivacy Proposal. However, Ecommerce Europe does not support the applicability of these restrictive rules on confidentiality also on permitted processing of electronic communications metadata. As already mentioned above, processing of non-personal confidential electronic metadata should be permitted on the same grounds as provided for by Article 6 of the GDPR. That is why Ecommerce Europe suggests amending Section 2 of Article 6 as follows:

> *2. Providers of electronic communications services may process electronic communications metadata:*
> *(a) on the same legal basis as provided for by Article 6 of Regulation (EU) 2016/679;*
> *or if:*
> *(b) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/212011 for the duration necessary for that purpose.*

In the view of Ecommerce Europe, the processing of electronic communication metadata, should exclusively be subject to the GDPR as far as personal metadata are processed. Such processing of personal metadata should thus only be possible on the legal basis provided for by Article 6 of the GDPR and with respect to its general principles. In the view of Ecommerce Europe, permitted processing, as far as personal metadata are concerned, are sufficiently covered by Article 6 of the GDPR.

Storage and erasure of electronic communications data: restrict Article 7 to Sections 1 and 2

Article 7 could, in the view of Ecommerce Europe, be restricted to the current Sections 1 and 2, as the duration of the storage of relevant electronic communication metadata for the purpose of billing, which is - per definition - about personal data, is sufficiently and equally covered by the provisions of the GDPR.

Protection of information stored in and related to end-users' terminal equipment: Article 8 should also be open for third party audience measuring

Ecommerce Europe believes that the meaning of "web audience measuring" is unclear. For instance, does it also include Wi-Fi networks? What does 'measuring' exactly mean? Ecommerce Europe asks for more clarification and better guidance on the meaning of this provision.

Ecommerce Europe also identifies some practical problems in the fact that the exception under d) is restricted to measuring carried out by the provider and is not extended to third parties. This is particularly problematic with regard to the current market for audience measurement. In practice, publishers often use third-party analytics to analyze their audience. The agreement between the publisher and the analytical partner (which may act as a subcontractor) assumes in principle that the data collected for the analysis cannot be used for purposes other than those foreseen in the binding agreement between the publisher and the third party.

In order to be effective and allow publishers to have a clear understanding of their web-based audience and to avoid undermining the audience measurement market, this provision should therefore also be open to web audience measuring carried out (on behalf of the publisher) by a third-party player. The current provision only allows the publisher of the site to perform such audience measurements on its own account using first party cookies exclusively. Consequently, the provision for measuring the audience on the Internet should not be limited to the publisher of the information society service requested by the end-users but also to its partners. That is why Ecommerce Europe welcomes amendments such as those proposed by the LIBE Rapporteur, MEP Lauristin, extending the provision also to third parties. Nevertheless, Ecommerce Europe regrets that the exception under d) is only limited to web audience measurement and believes that it as a missed opportunity not also allowing access to the terminal equipment of the end-user to improve the performance and quality of the requested information society service.

Moreover, Ecommerce Europe strongly recommends a new exception (subsection (e)) on behalf of repairing security, technical faults and/or errors in the functioning of information society services:

> *(e) it is necessary to maintain or restore the security of information society services, or detect technical faults and/or errors in the functioning of information society services, for the duration necessary for that purpose.*

With regard to Article 8, Section 2 (b), Ecommerce Europe would like to highlight the fact that the collection of information emitted by terminal equipment to enable the connection to another device will mostly take place in a public environment, such as cities, major roads, marketplaces and other parts of public space where the collection takes place. In that respect, Ecommerce Europe asks for clear guidelines on how (size and visibility) and where to display the information as meant in Article 8.2(b),

taking into account modern practical digital information techniques, such as active (deep) linking, network messaging and machine-readable barcodes as well as public safety and environmental care.

Improve the mechanism of consent for cookies and consent by browser settings

Consent definition and conditions for consent are the same as in articles 4 and 7 of the GDPR (unambiguous consent). Ecommerce Europe believes that it is, as such, consistent. A new element introduced by the proposal is that consent may also be given by appropriate technical settings of browser. Although Ecommerce Europe could overall support an opening of the consent mechanism to browser settings, it believes that the proposed provision does not represent the right solution to deal with the technical possibilities of giving appropriate approval or expressing consent for the use of cookies or the collection of information by browser settings. According to Ecommerce Europe, this restricted use of browser settings as a consent mechanism makes this instrument only fit for standard cookies used in a standard way, due to the incompatibility of preset browser settings and the requirement of specified detailed information before explicit consent is given. Therefore, Ecommerce Europe invites the European legislator to come up with a more practical solution to repair the impractical timeline for consent by browser settings caused by the prior specified information requirement.

Develop viable parameterization and avoid competition abuse in browser setting

Browsers can be considered as gatekeepers of the terminal (Recital 22 of the Commission's Proposal). Requiring browsers to prevent third parties from accessing the terminal equipment would have as a consequence that browsing software developers would become a power that is totally disproportionate to other players in the ecosystem of the Internet. The major players that develop browsing software (Google Chrome, Microsoft Internet Explorer, Apple Safari) - all established outside of the European Union - would be able to regulate standard access to the terminal equipment by browser setting consent systems, not only for themselves but also for their competitors. This would in fact allow these players to have a very favorable position, permitting them to use cookies necessary for the operation of the browser itself for all the services they provide on the web (search, advertising, audience analysis, etc.) and preventing competitors to benefit in the same way from the browser settings. In that perspective, Ecommerce Europe asks European legislators to come up with provisions that prevent the major publishers of navigation software to abuse browser setting consent systems to have a competition advantage or not complying with the European standards required by the GDPR.

Improve the provisions for unsolicited marketing communication (Article 16)

As the consent mechanism for e-mail marketing in the proposed Regulation has not changed compared to the one in the current e-Privacy Directive, Ecommerce Europe strongly advocates that existing standards developed by industry that meet the criteria of the Directive (as for instance, UFMD appendix to code for the use of personal data in direct marketing by electronic communication) are recognized as also meeting the standards of the new Regulation, thus giving the industry the necessary comfort of not having to develop new consent standards.

Under the e-Privacy Directive, the use of electronic contact details received in the course of a sales or service contract for unsolicited direct marketing e-mails is restricted to marketing for own similar products or services as they were subject to the sales or service contract on which occasion the e-mail address was gathered. In practice, it is highly problematic to assess which products or services fall within the scope of 'similar'. Moreover, traders have to file which products or services they sold to assess every time they sent a new unsolicited marketing e-mail whether they are allowed to do so without consent. This highly impractical practice is not only opposite to the GDPR obligation of data minimization, but it is also not well understood by customers, as they have a relation with the retailer and not with the good or service subject to the contract they concluded with the trader and, thus, expecting unsolicited offers on all the traders' products or services.

For the sake of simplicity and practicability and taking into consideration that the customer has always an easy and free of charge right to object (opt-out) unsolicited email marketing, Ecommerce Europe strongly recommends skipping the word "similar" from the text. This will allow the retailer to bring all his goods or services under the scope of this regulation, avoiding unnecessary data storing and complex discussions on what is seen as a similar product or service.

Ecommerce Europe

Rue de Trèves 59-61
B-1040 Brussel - Belgium
T. +32 (0) 2 502 31 34
www.ecommerce-europe.eu
www.ecommercetrustmark.eu
info@ecommerce-europe.eu
@Ecommerce_EU