ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN

WP 240

Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)

Adopted on 19 July 2016

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT OPINION:

SUMMARY

1. INTRODUCTION

The development of the digital market, alongside the recent adoption of Regulation 2016/679 (the General Data Protection Regulation or GDPR) calls for a thorough revision of the rules in Directive 2002/58/EC (the ePrivacy Directive or ePD). The revision of the ePD must lead to a regulatory system that is coherent and effective, and offers legal certainty as to what legal provisions apply in any particular situation. The ePD has, since 2002, provided a set of additional security and privacy measures with a particular focus on telephony and internet access providers. Article 1(2) of the ePD provides that this Directive was laid down to particularize and complement the Data Protection Directive 95/46/EC, which will be repealed by the GDPR when it will shall apply on 28 May 2018[1].

The Article 29 Working Party (WP29) supports the EC's recognition of the need to have specific rules for electronic communications in the EU. While the GDPR is a detailed legal elaboration of Article 8 of the Charter of Fundamental Rights of the European Union (the Charter) on personal data protection, Article 7 of the Charter specifically protects the confidentiality of communications. This human right equally deserves a detailed legal elaboration. The new legal instrument must supplement and complement the obligations of the GDPR in order to specifically protect the security of electronic communications.

The rules in the GDPR are always applicable to the processing of personal data, regardless of the nature of the data or the service provider(s). However the GDPR may not "*impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC*", according to its Article 95. The purpose of this provision, further developed in recital 173, is to ensure that the GDPR does not apply in cases where the ePrivacy Directive contains specific obligations with the same objective. However, in all other cases, the GDPR should apply. The current ePD already sets a high level of protection, by requiring the prior consent of users, before the collection of content from communications, traffic or location data, except in a limited number of cases. This consent requirement thus limits the possible legal grounds that can be used to justify the collection of personal data in the GDPR. In order to ensure consistency with Article 95 of the GDPR, the new ePrivacy instrument should at least maintain and reinforce its current principles, to guarantee the confidentiality of electronic communications. With regard to the legal ground, and without prejudice to the application of specific legal obligation justifying the data processing, it should be clear that the consent requirement prevails over the other legal grounds (such as the legitimate interest of the data controller) stated in Article 6 of the GDPR. Therefore, under the renewed ePrivacy instrument, service providers should only process information when this instrument - or another statutory provision referring expressly to it - permits it, or when the recipient of the service has given his prior consent.

The new ePrivacy legislation should provide additional rules to protect the security of electronic communications. This includes data generated by electronic communications

[1] Official Journal of the European Union, L 119, Vol. 59, 4 May 2016, URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

networks or systems that are not or are no longer personal data, and data processed by parties that cannot be considered data controllers or data processors. As a result, **the new instrument would provide additional protection to the electronic communications of natural and legal persons.**

Furthermore, since traffic, communication and location data are in most cases personal data, some overlap between the ePrivacy instrument and the GDPR is inevitable. In such cases the EC must ensure that besides a high level of confidentiality, the level of personal data protection in the GDPR is not undermined. **The revised ePrivacy instrument should keep the substance of existing provisions but make them more effective and workable in practice, by extending the scope of the rules on geolocation and traffic data to all parties, while simultaneously introducing more precisely defined conditions that take the intrusiveness of the processing of communication data to the private life of users thoroughly into account**.

Besides, the scope of the current ePD is mostly limited to traditional electronic communication services (such as internet service providers and telcos). Many of its provisions do not apply, for example, to Internet telephony (VoIP) or e-mail and instant messaging providers. Given the high dependence of many Europeans on electronic communications, **the new legal instrument must seek to protect the confidentiality of functionally equivalent electronic communication services** (such as, for example, WhatsApp, Google GMail, Skype and Facebook Messenger)**, especially when it concerns messages exchanged by and between individuals and private user groups.**

Another problem with the current ePD is the difference in interpretation of definitions, and thus differences in national legislation and enforcement. Different implementations are also the result of the discretion for Member States to decide whether certain restrictions of processing are optional (e.g. Article 12(3)) and on whether there are different obligations for individuals and business subscribers. The EC should aim to create a consistent legal regime across the EU, to ensure equal protection for individuals across EU Member States and a level playing field for all relevant actors in Europe. **As long as the revised ePrivacy instrument is clear and unambiguous in its definitions and requirements, then this aim could be met via either a Directive or a Regulation,** if there is very little margin of discretion for the Member States for national legislative activities regarding the level of protection.

2. SCOPE OF THE EPRIVACY INSTRUMENT

EXTENDING THE SCOPE TO NEW OTT SERVICE PROVIDERS

From the perspective of the user, there is a functional equivalence between means of communication such as traditional fixed-line telephony and internet services on the one hand, and telephony services over internet connections and mobile phone messaging apps on the other. As these services are using Voice over IP protocols, the acronym "VoIP" which in principle refers to the technology is often used as a shorthand for this type of services. But the legal protections in the ePD in principle only apply to providers of publicly available communications networks and services because the ePD rules were originally drawn up on

the premise that only transmission services should be covered by the framework, and higher-level services were considered to be outside this scope[2].

To introduce the issues further developed in Chapter 3, the current ePD in Article 5(1) essentially prohibits the interception of content and related traffic data in the core network (the telephony and internet access providers). Without strict rules, they would be able to monitor in real time the online activities of all their customers, and create detailed profiles, in particular because ISPs and telecommunications operators are in a position to handle all of their customers' communication data. **The obligations to respect the confidentiality of communication should equally apply to functionally equivalent new players on the communications market[3], such as virtual network operators and providers of communication services that are close substitutes to the corresponding services offered by telecom providers (e.g. unmanaged Voice over IP, instant messaging, webmail and messaging in social networks).**

Frequently, the word 'Over The Top' is used for these new services (OTT-services). But this word cannot be used without a clear legal definition and references to existing categories of communication services. In its report on OTT services[4], BEREC defines OTT service as "content, a service or an application that is provided to the end user over the public Internet", and divides these services in 3 categories:

- OTT-0 can be qualified as an Electronic Communication Service (ECS),
- OTT-1 is a service that does not fall under the current definition of an ECS but potentially competes with an ECS,
- OTT-2 are the other services, meaning any (other) information society service.

The EC should propose that the scope of the revised ePrivacy instrument includes all (or parts of) services, which allow individual communication and where service providers take the functional position of neutral carriers of the communication. The EC should identify potential legal gaps in the current situation, which pose a threat to the right to confidentiality of communications in general. **The EC should provide a clear definition of the functionally equivalent services that must comply with the confidentiality requirements,** especially

[2] More precisely, according to article 3, the ePD covers "*the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community*". These services should consist wholly or mainly in the conveyance of signals on electronic communications networks as opposed to e.g. the provision of content.

[3] The current differences in legal regime lead to unequal treatment of organizations, and untenable differences in the protection of fundamental rights of users, when data are processed in the context of very similar services (from a functional point of view) for similar purposes.

[4] BEREC Report on OTT services, January 2016 - BoR (16) 35, URL: http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5751-berec-report-on-ott-services_0.pdf.

when they meet the definition provided for the OTT-1 services, regardless of whether they can also be considered 'information society services'[5].

REVISING THE DEFINITIONS

The current European regulatory framework[6] for the online environment distinguishes three different categories of services: (1) information society services, (2) electronic communications services and (3) audiovisual media services. This distinction has been translated in the E-Commerce Directive, the Electronic Communications Regulatory Package and the Audiovisual Media Service Directive respectively.

In this regard, WP29 recalls its observation in Opinion 02/2008 **that the definitions of "public electronic communications network" and "electronic communications services" are very often unclear and do not reflect the infrastructure of today's communication networks.** These definitions do not take into account the blurring of the roles of network providers, virtual network operators and providers of communication services such as so-called OTT services (e.g. internet voice and chat providers). This issue has not been sufficiently addressed by the EC since the WP29 opinion of 2008, and continues to provide uncertainty to regulators and organizations.

In this respect, 'Information society services' are excluded from the scope of most provisions of the ePD[7]. If a provider of a functionally equivalent communication service is qualified as 'information society service', it would apparently not have to comply with the confidentiality requirements set down by the ePD. The different legal treatment of functionally equivalent services is a threat to the right to confidentiality of communications, and stands in the way of a level playing field. Therefore, the EC should identify these legal gaps, and evaluate and amend the definitions.

Though some of the rules in the ePD have been expanded to apply to all organizations carrying out certain activities – e.g. unsolicited direct marketing (Article 13) or accessing or storing information on a user's device (Article 5(3)), these specific extensions do not make up for apparent lacunae in the protection of communication secrecy in modern electronic communications and networks. While the Working Party recommends in general to extend

[5] Information society services would otherwise fall outside the scope of the revised ePrivacy instrument.

[6] Since the inception of this regulatory framework, the landscape of communications services has developed into a complex structure of interconnected networks and a wide variety of communication companies, some of which may be outside the EU.

[7] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.04.2002, p. 33, as amended by Directive 2009/140/EC and Regulation 544/2009. According to Article 2(c) of the Framework Directive the notion of "electronic communications service" does not include information society services, as defined in Article 1 of Directive 98/34/EC. In this regard, recital 5 of the Framework Directive recalls the need "*to separate the regulation of transmission from the regulation of content" and that the "framework does not therefore cover the content of services delivered over electronic communications networks using electronic communications services, such as broadcasting content, financial services and certain information society services"*.

the general scope of the new instrument to OTT-1 service providers, it also finds it necessary to expand the specific rules for location and traffic data to all organizations. Having such a varied scope is not a difficulty in itself, but the EC must ensure that any revision to the legislation provides for an unambiguous interpretation as to which organization must comply with a specific obligation.

ADDING 'PUBLICLY ACCESSIBLE PRIVATE' COMMUNICATION NETWORKS

The Working Party refers to the 2009 opinion[8] of the EDPS on the revision of the ePrivacy Directive which suggested including under the scope of application of the ePD "*the processing of personal data in connection with the provision of publicly available electronic communications services in public or* ***publicly accessible private communications networks*** *in the Community*" (emphasis added).

Such an expansion would bring all publicly available networks and services (wired or wireless, public or privately owned or managed) within the scope of the confidentiality requirements (for example Wi-Fi services in hotels, shops, trains, and networks offered by universities, corporate WiFi access offered to visitors and guests, hotspots created by individuals, etc.).

In this regard, WP29 would welcome any clarification about what should be considered as "publicly accessible" or not[9]. Only services which occur in an official or employment situation **solely** for work-related or official purposes, or technical communication between non-public bodies or public bodies solely in order to control work or business processes, as well as use of services for exclusively domestic purposes, may be exempted from the ePrivacy instrument. WP29 recommends that such examples be specified with an appropriate recital to provide guidance and clarity.

CONSEQUENCES FOR DATA RETENTION REQUIREMENTS

Due to concerns about imposing unnecessary or unwarranted data retention requirements, WP29 has previously been hesitant to impose obligations on a wider number of communications service providers. Given that Directive 2006/24/EC (the Data Retention Directive) has since been declared invalid by the CJEU[10], an important obstacle to include other actors than public providers of electronic communication services in the scope of the revised ePrivacy instrument has been removed.

The EC should explicitly state that it will not introduce any new European data retention requirement. Any similar retention of communications data in general must be prohibited in the revised ePrivacy instrument. The EC must ensure, when extending the scope of the new ePrivacy instrument, that this does not automatically allow Member States to bring new communication services in the scope of new or existing national data retention legislation. In

[8] EDPS 2nd Opinion on the revision of the ePrivacy Directive, January 2009, par 98, URL: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_EN.pdf

[9] For example, does this definition imply the impossibility to predict or even to know the identity of the users? In that case, does it exclude the users registered by the service or, for example, users on a guest list?

[10] Court of Justice of the European Union, Press Release No 54/14. Luxembourg, 8 April 2014, URL:http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdfhttp://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.

any case, the new ePrivacy instrument must specify that any national data retention laws must comply with the requirements of Article 8 ECHR and Article 51(1) of the Charter.

3. PROTECTING THE CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS

Protecting the confidentiality of communications (Article 5) is a key objective of the current ePrivacy Directive. This is also a core component of Article 7 (Respect for private and family life) and Article 8 (Protection of personal data) and Article 11 (Freedom of expression and information) of the Charter of Fundamental Rights of the European Union. Furthermore, a number of EU member states[11] recognize the secrecy of communications as a constitutional right.

REVISION OF ARTICLE 5(1)

When revising the ePrivacy rules, the new instrument should maintain a general prohibition of the interception/surveillance/monitoring of the content of electronic communications.

The EC should take into account the reasonable expectation of users that any communication provider is prohibited from unwarranted intrusion into their communications.

The revised Article must protect users against interception of the content of their communication regardless whether it concerns direct electronic communications between users or within a defined users group (e.g. a conference call or webcast), and protect users against the processing of their communications data. Such communications should be protected by the same degree of confidentiality as those within the current scope of the ePD, with the exception of content processed by the concerned users for exclusively domestic purposes.

The Working Party therefore encourages the EC to extend the application of article 5(1) to any service that is functionally equivalent to electronic communication services and networks. These services have in common that they enable the exchange of messages between a finite numbers of users. **To achieve this the EC could broaden the definition of "communication" laid down in Article 2(d) to explicitly include 'users' as defined in the current article 2(a), as in: "any information exchanged or conveyed between a finite number of parties or users",**

To avoid legal gaps in the protection of users, **the EC should elaborate in a Recital that interception and surveillance should be interpreted in the broadest technological meaning, including the injection of unique identifiers such as, for example, advertising identifiers, audio beacons or super cookies to (the content of or traffic data related to) the communication**.

The Working Party also recommends the inclusion of a **clarification of the definitions of 'communications data' and 'related traffic data'.** The current phrasing in Article 5(1) of the ePrivacy instrument has caused confusion about the meaning of the prohibition on the interception or surveillance of 'communications and related traffic data' in Article 5(1), and

[11] e.g. Germany Art. 10 Grundgesetz (Secrecy of Communication).

the separate rules for the processing of traffic data in Article 6. The historical distinction between content and metadata is no longer so clear-cut. With plain old telephony, a clear line could be drawn between interception of the call itself, and the traffic data (who called whom, and when).

Digital communication is governed by technical protocols that do not necessarily distinguish between the contents of communication and related traffic data. For example the http protocol prescribes the use of URL's that contain both elements of content (visited webpages which content can be read from the URL's anchor and parameters) and traffic data (host names). Hence it has become increasingly difficult to apply the separate legal definitions for traffic data and for communications data, for example especially when a network provider engages in packet inspection and the analysis reveals the contents of communication between users and third parties (the visited URL's).

The Working Party notes that the transposition of data retention legislation by Member States has also led to different interpretations of these essential definitions, thus causing regulatory uncertainty. Therefore the Working Party invites the EC to **illustrate with clear examples when the confidentiality rules for communications and related traffic data (currently in Article 5(1) of the ePD) have to be applied, and when the specific rules for traffic data are to be applied exclusively (currently in Article 6 of the ePD**). This is also relevant in circumstances where providers of publicly available communication networks offer publicly available communication services themselves (such as mobile telephony, digital TV, Pay per Event and Video on Demand) and may collect and store data related to the use of these services that reveal information about the content of the communications, such as visited URL's. **The Working Party recommends to provide an extensive list in a specific recital.**

In general, the EC should specify that the GDPR requirements on purpose limitation and data minimization apply. The processing of the content of communications and related traffic data can only be legitimate as long as it is performed for a specific legitimate purpose and if the categories and volume of data to be processed are kept to the minimum necessary for the delivery of the requested service. As a general rule, even if an exception applies that allows for the interception of the communication, the data should be deleted or irreversibly anonymized as soon as possible. The EC must provide a clear explanation (along the lines of Opinion 5/2014 of WP29 on anonymization techniques) that data are not anonymous as long as the operator still has the original data for another purpose.

In addition, the current exception on the consent requirement for 'lawful business practices' is not precise enough. It must be clear that use of the data for advertising, marketing, 'product innovation' or research purposes should never be allowed to override the requirement of prior consent for the interception of the content of communication and related traffic data.

In order to take into account some legitimate use of content data, especially when it comes to securing the service provided to the users, the EC could create the following 2 exceptions on the consent requirement:

1. Transmission: If the data are technically strictly necessary for the transmission of electronic communication requested by a user. It should be absolutely clear that the delivery

of advertising, and use of the data for marketing, research and audience measurement are not strictly necessary to deliver a service that is requested by a user.

2. Security: If the processing is strictly necessary to proactively and defensively maintain and manage the security of a network or service (including network forecasting, detecting and solving incidental or structural problems, spam, malware, spyware and data breach detection, solution and prevention). Any recordings of content data have to be deleted immediately when they are no longer necessary for this purpose.

The EC should specify that the GDPR requirements on proportionality and subsidiarity apply in any case; regardless of whether consent is required, or if any of the exceptions are invoked.

REVISION OF ARTICLE 5(3)

While keeping the consent requirement in the current Article 5(3) of the ePD, the rules should be rephrased to better protect the confidentiality of the communication devices of users. The current phrasing of the consent requirement for 'the storing of information', or the 'gaining of access to information already stored' in the terminal equipment (communication devices) of users, has created ambiguity as to its applicability.

The revised Article 5(3) should be rephrased as technologically neutral as possible. Tracking techniques used on smartphones and Internet of Things applications should be considered when defining the actions covered by the revised Article 5(3), especially when it comes to 'passive tracking', that is, the use of identifiers and other data broadcast by devices. For example, in order to set up communications with a WiFi access point, smartphones continually broadcast their MAC-address. These signals may be captured and processed for a different purpose than to carry out transmission of communication, such as counting visitors, or even creating detailed location patterns over time and across locations. With the development of Internet of Things, more and more data could be transmitted 'by default' for technical reasons, but used for intrusive purposes (notably marketing purposes) not related to the initial purpose of the broadcasting. In short, **the rules governing the collection of information from user devices should not depend on the kind of device owned by the data subject nor on the technology employed by an organization**, especially with regard to the use of information for marketing and market analysis purposes.

The EC should also clarify that data do not necessarily have to be stored inside of the terminal equipment, but can also be processed (including collected and stored) elsewhere and made available through the device, and in these situations Article 5(3) will apply. However, while clarifying the broad scope of the consent requirement, the EC should also create more specific exceptions, to allow for the processing of data that causes little or no impact on the rights of users to secrecy of communications and private life.

The Working Party has already called on the EC (opinion 04/2012 on Cookie consent exemption) to create a new exception for first party analytic cookies which "*are not likely to create a privacy risk when they are strictly limited to first party aggregated statistical purposes*". Such practice is allowed under the condition that websites "*provide clear information about these cookies in their privacy policy as well as adequate privacy safeguards*" such as "*user friendly mechanism to opt-out from any data collection and*

comprehensive anonymization mechanisms that are applied to other collected identifiable information such as IP addresses"[12].

In view of the rapid development and deployment of new ways to track users through information stored in, or broadcast by their devices, the exception should not be limited to a particular technique, but focus on the impact on users' privacy and right to secrecy of communications.

There should be at least 2 exceptions on the consent requirement:

1. Transmission (the current exemption should remain)- if the data are technically strictly necessary for the technical transmission of electronic communication requested by a user. It should be absolutely clear that the delivery of advertising, and use of the data for marketing, research and audience measurement are not strictly necessary to deliver a service that is requested by a user.

2. Security - if the processing is strictly necessary to proactively and defensively maintain and manage the technical security of a network or service, including network forecasting, detecting and solving incidental or structural problems (also to provide customer service in this respect), spam, malware, spyware and data breach detection, solution and prevention.

Additionally, the Working Party invites the EC to consider other circumstances in which consent would not be required, because the processing would have little or no impact on the right of users to protection of their communication secrecy and private life.

Such circumstances could be:

1. Anonymization - if the data are immediately and irreversibly anonymized during collection on the device, or on the endpoints of the network/sensors. It must be clear that this exception cannot apply as long as the provider of the service, or a third party with whom the provider jointly provides a service, still has access to the original data that are stored for another purpose. Hence consent would still be required if the data are simply hashed, aggregated or otherwise pseudonymized, but there remains a possibility to link events in the aggregated data to the original data, also if future reading of information from a device creates linkability to events in the aggregated data set.

2. When the data collection is limited by design to have little or no impact on the right to privacy and confidentiality of communications. This exception can only be invoked under the following (cumulative) conditions:

- The data collection is strictly limited to statistical analysis of the quality of the delivered service by the natural or legal person, public authority, agency or other body that determines the purpose and the means of the service ("first party")13. If a

[12] In short, WP29 has promoted the insertion of a "third exemption criterion to consent for cookies that are strictly limited to first party anonymized and aggregated statistical purposes".

[13] The Working Party notes in its Opinion on the Cookie Consent Exemption (p. 11): "*First party analytics should be clearly distinguished from third party analytics, which use a common third party cookie to collect navigation information related to users across distinct websites, and which pose a substantially greater risk to privacy.*"

third party is involved in the technical collection of the data, the exception may only be invoked if that party has signed a processor agreement as defined in Article 28 of the GDPR and the agreement prohibits any further use of the collected data by the processor for any other purpose. This exception cannot be invoked for the analysis of location data.

- The collection takes place in a restricted and single area. This excludes the tracking and profiling of users (based on the collection of information stored in, or broadcast by their devices) across different locations and/or different domains or services.
- The user is to be provided with prior and adequate information about the collection and the purposes, as defined in Articles 12-14 of the GDPR.
- A user friendly mechanism is proposed to opt-out from any further data collection, without creating new privacy risks.
- The collection and processing of the information serve a legitimate purpose, comply with the principles of proportionality and subsidiarity so that they are designed to have limited impact. This can be achieved, depending on the circumstances, by using samples instead of the full dataset, keeping the categories and volume of collected data to the minimum necessary for this specific purpose, and/or by applying comprehensive anonymization mechanisms to the collected data after a limited period of time.
- The data processed do not constitute data of a sensitive nature and special categories of personal data under Art. 9 GDPR (including for example data about areas or communication partners from which sensitive data may be inferred).

With regard to the first exception, the information provided to users can be limited to a general description of this purpose, but with regard to the second exception and other circumstances in which consent would not be required, the revised ePrivacy instrument must specify that users must be informed about the categories of data and purposes of the processing.

The Working Party would welcome a clear legal definition of the purposes of data processing which do not require consent. In addition, the Working Party advises the EC to refer to future guidance to be provided by the EDPB.

MERGER OF ARTICLES 6 AND 9 (TRAFFIC AND LOCATION DATA)

Different from the protection of the pipeline in Article 5(1), the scope of Article 5(3) is extended to all parties breaching the confidentiality of information stored on the device. However, Articles 6 and 9 of the ePD on the processing of traffic and location data yet again only apply to the traditional 'pipeline' providers, not to other parties processing these data.

The European Court of Justice has acknowledged in recent rulings that metadata about communications can provide an intrusively revealing picture of a person’s interests and whereabouts. These data are no longer only collected by traditional ISPs and telephony providers, but by many different organizations, also outside of the EU. These new service providers, such as app developers, may also obtain a very detailed overview of a users' travel and communication patterns, while they may not be subjected to the obligations of the current ePD (as long as they don't read information stored in the terminal equipment of users). Additionally, through these new services, the boundaries between traffic and location data have become blurred.

Based on the recurrent observation of location data, travel patterns may be revealed, including home addresses and work addresses. Traffic data such as calling behavior may reveal social patterns and relations between users while website traffic data may reveal sexual orientation, or for example political affiliation.

Even if some or parts of the communications data are immediately deleted from the dataset after collection, the collection of traffic and location data over time and/or across different platforms/domains/services may result in individual or group profiles or statistics that can be used to treat people differently. Such types of tracking thus have a high impact on the private life of users and justify the need for a prior consent.

By merging the provisions in the current ePD on traffic and location data, the revised ePrivacy instrument may set a clear rule for all parties. By requiring consent for the processing of all these metadata, the revised ePrivacy instrument shall offer a high level of protection, using a legal basis as strong as the consent of the data subject, stated in Article 6 of the GDPR. The confidentiality of communication is a core right for a democratic society. Therefore, the confidentiality of communications and related metadata require stricter rules, especially because modern communication technologies enable massive collection of intrusive data with covert techniques, or at least techniques people are not fully aware of. The collection, processing and use of these data for other purposes than providing the communication must be exceptional and must only be allowed after users have been adequately informed and have provided consent.

In order to better protect the secrecy of electronic communications, the Working Party therefore advises the EC to create a harmonized consent requirement for the processing of metadata such as traffic and location data. This consent requirement should apply to all traffic and location data, also when they are generated through sensors in a user device. The new rule should apply to all parties collecting and processing these data.

The definition of consent is currently provided by the Directive 95/46/EC, according to the Article 2 of the ePrivacy Directive. The new ePrivacy instrument should as well use the definition of the data subject provided in Recital 32 and Article 4(11) of the GDPR and meet the conditions set in recital 42 and Article 7, especially regarding its form and the data controller's ability to produce the evidence of such consent. While clarifying the broad scope of the consent requirement for traffic and location data, the EC should also create more specific exceptions, to allow for processing of data that causes little or no impact on the rights of users to secrecy of communications and private life.

As the Working Party noted in Opinion 04/2012, not all uses of technology falling within the scope of Article 5(3) present a privacy risk to users. Similarly, when network operators and service providers process the traffic and location data that are necessary to technically deliver a requested service (only for that purpose), such processing does not necessarily pose a high risk to users. Other relevant examples of such processing with a low privacy risk to users are the processing for billing purposes and for specific security purposes, such as detecting malware, spam, botnets, fraud or data breaches, assuming this processing complies with the requirements of transparency, proportionality, and adequate safeguards are in place to protect the rights and interests of the individuals concerned.

Following this approach of distinguishing purposes between the impacts they have on user's rights, there should be at least 3 exceptions on the consent requirement:

1. Transmission - if the data are technically strictly necessary for the transmission of electronic communication requested by a user. It should be absolutely clear that the delivery of advertising, and use of the data for marketing, research and audience measurement are not necessary to deliver a service that is requested by a user.
2. Security - if the processing is strictly necessary to proactively and defensively maintain and manage the security of a network or service (including network forecasting, detecting and solving incidental or structural problems (also to provide customer service in this respect), fraud, spam, malware, spyware and data breach detection, solution and prevention).
3. Billing - if the processing of location and traffic data is strictly necessary for (keeping evidence of) billing/electronic transactions. This exception should not allow parties to send bills for 'free' services, to process data that would otherwise require consent of the users.

Additionally, the Working Party invites the EC to consider other circumstances in which consent would not be required, because the processing would have little or no impact on the right of users to protection of their communication secrecy and private life.

Such circumstances could be:

1. Anonymization - if the data are immediately deleted or irreversibly anonymized after the transmission of a communication has been completed. It must be clear that this exception cannot be invoked as long as the provider of the service, or a third party with whom the provider jointly provides a service, still has access to the original data that are stored for another purpose. Hence consent would still be required if the data are simply hashed, aggregated on an event level or otherwise pseudonymized, but there remains a possibility to single out users, or linkability of individual events in the aggregated data to the original data, also if future collection of traffic or location data creates linkability to events in the aggregated data set.
2.
3. When the data collection and (further) processing is limited by design to have little or no impact on the right to private life and confidentiality of communications. This exception can only be invoked under the following (cumulative) conditions:
4. The user is to be provided with :
5. prior and adequate information about the collection and the purposes as defined in the Articles 12-14 of the GDPR.
6. with regard to location data: a user friendly mechanism is proposed to opt-out from any further data collection
7. The collection and processing of the information serve a legitimate purpose, comply with the principles of proportionality and subsidiarity so that they are designed to have limited impact. This can be achieved, depending on the circumstances, by using samples instead of the full dataset, keeping the categories and volume of collected data to the minimum necessary for this specific purpose, and/or by applying comprehensive anonymization mechanisms to the collected data after a time period which should be limited to what is strictly necessary.

8. The data processed do not constitute data of a sensitive nature or special categories of personal data under Art. 9 GDPR (for example data about areas or communication partners from which sensitive data may be inferred).

With regard to the second and third exception, and other circumstances in which consent would not be required, the revised ePrivacy instrument must specify that users must be informed about the data and the purposes of the processing.

Once the provisions on location data and on traffic data are merged, there would no longer be a need for the specific current exceptions for marketing and for 'value added services'.

CONSIDERATION REGARDING USER CONSENT REQUIRED IN THE EPRIVACY INSTRUMENT

WP29 has provided extensive guidance on the consent requirement in respect of cookies and similar technologies in Opinion 04/2012[14], Working Document 02/2013[15] and Opinion 9/2014[16]. WP29 has also provided general guidance on consent itself in Opinion 15/2011[17].

The prior consent of the user should remain a key principle in the new ePrivacy instrument, regarding the collection of metadata, content data, and tracking techniques. To ensure consistency with the GDPR, the new instrument should clearly refer to the GDPR provisions, specifying the definition, conditions and forms of the consent.

On the one hand, given the sensitive nature of communications data, consent is the preferred legal ground, to enable users to determine, based on adequate information, whether they allow the proposed processing for a specific purpose. On the other hand, WP29 notes that in many instances, industry has developed consent mechanisms with the objective of arguably meeting the bare legal requirements for compliance but that fail to give users a free choice regarding this processing. This is the case with so-called cookie walls. These mechanisms in effect lead to the denial of access for those users that do not accept cookies, also when it concerns tracking cookies with a commercial purpose, with high privacy risks for users.

These "take it or leave it" approaches rarely meet the requirements for freely given consent, as defined in the 95/46/EC Directive and, in particular, Recital 43 of the GDPR. In its opinion on consent, WP29 specifically stated that "*if the consequences of consenting undermine individuals' freedom of choice, consent would not be free*". The Working Party invites the EC to develop a specific prohibition on such 'take it or leave it' choices with regard to electronic communications, where such choices would undermine the principle of freely given consent.

[14] WP 29, WP 194, Opinion 04/2012 on Cookie Consent Exemption, URL:http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.
[15] WP 29, WP 208, Working Document 02/2013 providing guidance on obtaining consent for cookies URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.
[16] WP 29, WP 224, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf.
[17] WP 29, WP 187, Opinion 15/2011 on the definition of consent, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

The Working Party has identified 5 circumstances in which forced consent should be specifically prohibited and users must be given a free choice to accept or deny the processing and still use the service, namely:

1. Tracking on websites, apps and or locations that reveal information about special categories of data (health, political, sexual, trade union etc.). Even if visits to services providing information about such special categories of data do not disclose in themselves special categories of data about these users, there is a high impact on the private life of those users if they are labelled as being interested in such information;

2. Tracking by unidentified third parties for unspecified purposes. This is for example the case when a website or app auctions its advertising space, and unknown third parties may actually start to track the users through the website or app;

3. All government funded services;

4. All circumstances identified in the GDPR that lead to invalid consent, such as for example an unequal balance of power, if there is no equivalent alternative, or forced consent is part of a contract;

5. Bundled consent for processing for multiple purposes. Consent should be granular.

The Working Party calls on the EC to pay special attention to the position of news media, since they seem to be the heaviest users of tracking cookies and cookie walls[18]. There is a clear democratic need to ensure the economic survival of news media. However the EC should not accept that news media impose invasive tracking of users.

When consent is the applicable legal basis, users must be provided with truly easy (user friendly) means to provide and revoke consent. **The Working Party recommends rephrasing the requirements in the current Recital 66 of Directive 2009/136/EC. Instead of relying on website operators to obtain consent on behalf of third parties** (such as advertising and social networks), manufacturers of **browsers and other software or operating systems should be encouraged to develop, implement and ensure effective user empowerment, by offering control tools within the browser** (or other software or operating system) such as Do Not Track (DNT), or other technical means that allow users to easily express and withdraw their specific consent, in accordance with Article 7 of the GDPR. Such tools can be offered to the user at the initial set-up with privacy-friendly default settings. Adherence to accepted technical and policy compliance standards must become a common practice. In addition, website operators should respect and adhere to browser control tools or other user preference settings.

4. PROTECTING THE SECURITY OF ELECTRONIC COMMUNICATIONS

[18] Recent research from Steven Englehardt and Arvind Narayanan from Princeton University, Online tracking: A 1-million-site measurement and analysis, Draft: May 18, 2016. See for example URL: http://motherboard.vice.com/read/news-sites-are-tracking-your-web-traffic-way-more-than-porn-sites.

The key purpose of the security article in the revised ePrivacy instrument (now Article 4 of the ePD) should be to not only protect the security (in particular the confidentiality) of communications while in transit or stored, but also to protect the security of end user equipment. This should be specified in the text of the legislation and not only in a recital (now Recital 24 of the ePD). The Working Party recommends including a direct reference to the security obligations in the GDPR (as stated in its Article 5 and Article 32).

The EC should carefully assess whether the expanded consent requirements in the revised ePrivacy instrument do not prevent legitimate processing for necessary security purposes[19].

The revised security article should also specifically protect end user devices against spyware (malicious unsolicited access to communication data stored on, or generated by, the device or the storing of information on an end user device, including software preloads or unsolicited pushed information).

The Working Party endorses the inclusion of the following proposals in the Public Consultation on the Evaluation and Review of the ePrivacy Directive from the European Commission[20]:

- Development of minimum security or privacy standards for networks and services;
- Extension of security requirements to reinforce coverage of software used in combination with the provision of a communication service, such as the operating systems embedded in terminal equipment. For example, mandatory updates may be provided, but the user should be adequately alerted about new security risks, and enabled to easily update the OS him or herself;
- Extension of security requirements to reinforce coverage of Internet of Things devices, such as those used in wearable computing, home automation, vehicle to vehicle communication, and
- Extending the security requirements to reinforce coverage of all network components, including SIM cards, apparatus used for the switching or routing of the signals, etc.[21]

The Working Party also invites the EC to provide further guidance with regard to the implementation of the essential data protection principles of Privacy by Design, and Privacy by Default as referenced in Recital 78 of the GDPR[22].

---

[19] For example, the Article 29 Working Party has already considered in Opinion 1/2009 that email providers can use filtering systems in order to detect viruses, considering their obligation to take appropriate technical and organisational measures to safeguard the security of their services, in accordance with the security obligation set up in Article 4 of the ePD.

[20] EC, Public Consultation on the Evaluation and Review of the ePrivacy Directive, URL: https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive.

[21] See also the report from the Federal Trade Commission (2016): 'ASUS settles FTC charges that insecure home routers and "cloud" services put consumer's privacy at risk'. 23 February 2016, URL: https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

Privacy by Design and Privacy by Default should also apply to network providers, providers of network components, terminal (including IoT) or complementary equipment (including software) used in combination with the provision of electronic communications services[23]. When implementing the Privacy by Design and Privacy by Default principles, parties should focus on the provision of granular choices, enabling individuals to use a "do not collect" option to schedule or quickly disable any collection, the prevention of location tracking, (for example by disabling wireless interfaces when they are not used or by using random identifiers), to enforce transparency and user control, and limit as much as possible the amount of data leaving devices by transforming raw data into aggregated data directly on the device.

Besides, **the Working Party invites the EC to consider protecting the rights of users to use encryption to protect their electronic communications.** Such a rule might also include the development of technical standards on encryption, also in support of the revised security requirements in the GDPR. Encryption has grown into a critical tool to protect the confidentiality of communications within electronic communications networks. The use of encryption has increased after the revelations about efforts by public and private organizations and governments to gain access to communications. But at the same time, governments are trying new ways to gain access to encrypted communications. The Working Party would welcome new obligations to use algorithms and standards that have proven to be secure, to respect the confidentiality of encrypted communications and to prohibit the decryption, reverse engineering or other monitoring of those communications protected by encryption, with a limitative description of exemptions.

5. DELETION OF SPECIFIC DATA BREACH RULES

WP29 recommends deleting the Articles 4.2 and Articles 4.3 of current ePD. The GDPR already obliges all data controllers, including providers of publicly available electronic communications services, to notify subscribers and competent national authorities of a personal data breach (subject to certain exemptions). To avoid duplicate notifications, the process must be simplified and all data breaches involving personal data should be notified to the supervisory authorities provided for in GDPR, using the trigger thresholds set out in that instrument.

---

[22] This Recital states that "*when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders*".

[23] Standardization is a concrete answer to practical questions raised by the implementation of the consent and choice mechanism, regarding internet tracking (art.5(3)) and the collection of traffic and location data (art. 5(1), 6 and 9), following the example of the work carried out by the W3C and WP29 regarding the DNR Compliance Specifications

6. HARMONISATION OF PROVISIONS ON UNSOLICITED COMMUNICATIONS

The current rules in the ePD concerning unsolicited communications aim to protect users against the annoyance and costs of receiving unsolicited communications.

The means by which unsolicited communications are conducted have evolved since the ePD first came into force. As an example, an unsolicited communication can start with an automated dialer, play a recorded message and then use a chat-bot to interact with the called individual via a series of automated screening questions. The chat-bot can then use the answers to transfer the called individual to a live operator.

Therefore, WP29 recommends that the rules on unsolicited communications are rephrased to take new developments into account. The revised Article 13 of the ePrivacy instrument should require the prior consent of recipients for all types of unsolicited communications, independent of the means (e.g. electronic mail, behavioral advertising, voice or video calls, fax, text and direct-messaging). The burden of proof of obtaining the consent (of either legal or natural persons) should be on the sender or the party commissioning the unsolicited communication, including keeping time stamped copies of the information provided to users when obtaining the consent.

Users must be able to revoke such consent easily and free of charge, via simple means that have to be indicated in each subsequent communication. The recipient should be able to revoke consent at any time and without stating a reason. In line with Article 7(3) of the GDPR, it should be as easy to withdraw consent as to give it. Any commercial purpose of the communication should be clearly identified at the beginning of the communication.

Users must be able to express and revoke consent across industries or particular sectors in an easy and user-friendly way. Where possible, they should be able to do this through their browsers or other software or operating systems. Given the limitations of providing and withdrawing consent on an individual basis, the Working Party recommends the creation of registers or other systems that provide an effective solution for a user-friendly revocation of consent or reset of marketing preferences across a range of organisations or particular sectors. To reflect Article 7(3) of the GDPR it is particularly important to give an easy one-stop mechanism for withdrawing consent to third party marketing where contact details have been included on marketing lists sold on to large numbers of unknown third parties.

The consent has to be specific, as defined in Article 7 of the GDPR. If consent is sought for inclusion in marketing lists to be used by third parties, such consent can only be legally valid if it is separated from, and not combined with, the consent for the first party communication. The categories of products for which electronic communication may be sent and the (categories of) recipients have to be clearly described before obtaining the consent[24]. This requirement also applies to so-called 'hosted' communications, where an organization sends unsolicited communication on behalf of other organizations (for example e-mail or targeted advertising in social networks).

[24] In line with WP29 WP 174 Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing.

Additionally, the exception in Article 13(2) of the current ePD for existing customers should be limited to a reasonable level of marketing communication. Parties should not be allowed to bombard users with an excessive number of marketing calls or messages. Also, the definition and scope of "similar products and services" would benefit from clarification.

7. HARMONISATION OF PROVISIONS ON DIRECTORIES OF SUBSCRIBERS

In Article 12 the ePD provides the right to subscribers to "*determine whether their personal data are included in a public (printed or electronic) directory.*" The wording of this article refers to a time where paper copies of telephone directories were distributed to every household, and when people dialed directory enquiry services. The wording of this article creates legal uncertainty as to whether equivalent services from social networking or other information society services are within scope.

This article therefore requires modernization and clarification. Given the prevalence of networking and messaging services in today's society, WP29 recommends to include all kinds of directory services in the scope, in addition to types of services which exist to simply consolidate the directories of other services. Additionally, the consent requirement for 'reverse lookup' in the current Article 12 (3), should explicitly apply to other service identifiers such as an email address or user name.

8. CALL LINE IDENTIFICATION (CLI)

The ePD includes an important right for call recipients to be informed about who is calling them and take action against those calls which withhold their CLI. Some Member States have also strengthened the protection in this area by legislating that all outgoing marketing calls must display a valid CLI[25]. It is important that the integrity of CLI information transmitted between interconnecting networks is maintained such that a user's request to display or withhold CLI is maintained and also to ensure that it cannot be spoofed or falsified.

The Working Party recommends a rewording of Article 8 of the ePrivacy instrument to reflect these developments.

[25] For example, in the UK, Regulation 10 of the Privacy and Electronic Communications Regulations (which implement the ePD in the UK), URL: http://www.legislation.gov.uk/uksi/2003/2426/regulation/10/made

9. ENFORCEMENT

To promote a harmonized interpretation, the GDPR creates new obligations for the supervisory authorities, such as cooperation between competent national authorities, the consistency mechanism and the role of the European Data Protection Board.

The present ePD allows for the situation where more than one administrative body can act as competent supervisory authority. Supervision of the new ePrivacy instrument should in any case provide for a homogeneous governance model which allows for effective cooperation mechanisms between supervisory authorities. Secondly, in situations where more than one administrative body can act as the competent supervisory authority, sanctions should be harmonized to match with the sanctions provided in the GDPR.

In practice these situations will mostly also include the processing of personal data, thus creating overlap in supervision. Therefore the Working Party advises the EC to determine that the national data protection authorities are the competent authorities with regard to the new ePrivacy framework in order to ensure a consistent and coordinated regulation and enforcement.