P

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 5/2016

Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC)

EDPS

22 July 2016

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '...for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and foster accountable policymaking - in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'.

Executive Summary

This Opinion outlines the position of the EDPS on the key issues relating to the review of Directive 2002/58/EC on privacy and electronic communications (the ePrivacy Directive)[1], in response to a request of the European Commission.

We need a new legal framework for ePrivacy, but we need a smarter, clearer and stronger one: we need more clarity but also better enforcement. We need it to ensure the confidentiality of our communications, a fundamental right enshrined in Article 7 of the Charter of Fundamental Rights of the European Union. In addition, we also need provisions to complement, and where necessary, specify in more detail, the protections under the General Data Protection Regulation (GDPR). Furthermore, we also need to maintain the current, higher level of protection where the ePrivacy Directive provides more specific safeguards than the GDPR. The definitions of the GDPR, its territorial scope, the mechanisms for cooperation between enforcement authorities and for consistency, as well as the possibility to provide flexibility and guidance, should be available for ePrivacy.

The scope of the new legal framework must be extended. This is to take account of technological and societal changes and to ensure that individuals be afforded the same level of protection for all functionally equivalent services, irrespective whether they are provided, for example, by traditional telephone companies, by Voice over IP services or via mobile phone messaging apps. Indeed, there is a need to go even further and protect not only 'functionally equivalent' services, but also those services that offer new opportunities for communication. The new rules should also unambiguously continue to cover machine-to-machine communications in the context of the Internet of Things, irrespective of the type of network or communication service used. The new rules should also ensure that the confidentiality of users' communications will be protected on all publicly accessible networks, including Wi-Fi services in hotels, coffee shops, shops, airports and networks offered by hospitals to patients, universities to students, and hotspots created by public administrations.

Consent should be genuine, offering a freely given choice to users, as required under the GDPR. There should be no more 'cookie walls'. Beyond a clear set of exceptions (such as first party analytics), no communications should be subject to tracking and monitoring without freely given consent, whether by cookies, device-fingerprinting, or other technological means. Users must also have user-friendly and effective mechanisms to provide and revoke their consent within the browser (or other software or operating system).

In order to better protect the confidentiality of electronic communications, the current consent requirement for traffic and location data must also be maintained and strengthened. The scope of this provision should be broadened to cover everyone and not just traditional telephone companies and internet service providers.

The new rules should also clearly allow users to use end-to-end encryption (without 'back-doors') to protect their electronic communications. Decryption, reverse engineering or monitoring of communications protected by encryption should be prohibited.

Finally, the new rules on ePrivacy should protect against unsolicited communications and should be updated and strengthened, requiring prior consent of recipients for all types of unsolicited electronic communications, independent of the means.

TABLE OF CONTENTS

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty of the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular Articles 28(2), 41(2) and 46(d) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION AND BACKGROUND

This preliminary Opinion (Opinion) is in response to a request of the European Commission (Commission) to the European Data Protection Supervisor (EDPS), as an independent supervisory authority and advisory body, to provide an opinion on the review of the ePrivacy Directive[2].

The consultation of the EDPS was carried out in parallel with a public consultation held by the Commission, which was open until 5 July 2016[3]. The Commission also requested the opinion of the Article 29 Data Protection Working Party (WP29), to which the EDPS contributed as a full member[4].

This Opinion contains the preliminary position of the EDPS on the review of the ePrivacy Directive, focusing on those issues where his opinion has been specifically requested by the Commission. The Opinion also constitutes the EDPS contribution to the public consultation and as such, may also address other issues not specifically requested by the Commission in its request for an opinion. We may also provide further advice in subsequent stages of the legislative procedure.

The review of the ePrivacy Directive is one of the key initiatives of the Digital Single Market Strategy[5], aimed at reinforcing trust and security in digital services in the EU with a focus on ensuring a high level of protection for citizens and a level playing field for all market players across the EU.

The review seeks to modernise and update the ePrivacy Directive as part of the wider effort to provide a coherent and harmonised legal framework for data protection in Europe. The ePrivacy Directive particularises and complements Directive 95/46/EC[6], which will be replaced by the recently adopted General Data Protection Regulation (GDPR)[7]. The ePrivacy Directive sets forth specific rules, with the main objective of ensuring the confidentiality and security of

electronic communications. It also protects the legitimate interests of subscribers who are legal persons.

II. NEED FOR A NEW LEGAL INSTRUMENT FOR ePRIVACY

The EDPS supports the Commission's initiative to modernise, update and strengthen the provisions of the ePrivacy Directive. We share the view, also expressed by the WP29 in its recent opinion[8] as well as by civil society groups in their recent joint analysis[9], that there is a continued need to have specific rules to protect the confidentiality and security of electronic communications in the EU and to complement and particularise the requirements of the GDPR. We also believe that we need selective and targeted legal provisions that provide strong, smart and effective protection.

The existing ePrivacy Directive provides protection in areas which are not covered by the concept of processing of personal data, which is the condition for the applicability of core data protection instruments such as Directive 95/46/EC or the GDPR. It provides for more precise rules in specific processing situations, where the potential impact of the processing is important. Furthermore, it considers actions for which the processing of personal data is not necessarily the main factor of concern for the individual, e.g. the transmission of unsolicited messages.

II.1 Confidentiality of electronic communications must remain protected

The right to the confidentiality of communications is a fundamental right protected under Article 7 of the Charter of Fundamental Rights of the European Union (the Charter) - the modern-day equivalent of traditional (postal) statutes guaranteeing the secrecy of correspondence[10]. The ePrivacy Directive is the only instrument in EU secondary law that comprehensively implements Article 7 of the Charter.

Furthermore, the Directive goes beyond implementing Article 7 and particularising data protection rules for a specific economic sector. It also protects legitimate interests of legal persons with respect to confidentiality of communications. With new developments, including the ever-increasing amount of electronic communications, increasing surveillance of these communications by public and private entities, and new technological developments such as cloud computing, Internet of Things and Big Data, it is becoming ever more important to protect the confidentiality of communications.

Confidentiality of communications is essential for the functioning of modern societies and economies: without trustworthy messengers who deliver information to the recipients without using it for own purposes, disclosing it to third parties, modifying the content, suppressing or delaying the delivery, business could only be conducted face to face. The ePrivacy Directive obliges all electronic communications providers to be trustworthy messengers and saves individuals and organisations from the need to find out who can be relied upon for communications services and who can't. This applies today and should continue to apply to all communications, regardless of the sender, the recipient and the content. Indeed, the content of a communication should normally be unknown to the communications provider.

While the economic and social importance of trustworthy communications cannot be overstated, the protection of the fundamental right to privacy against any interference, especially from state authorities, is its central legal function.

In order to ensure legal certainty, it is crucial to have clear and specific legal rules in secondary legislation to put into practice the principle of confidentiality of electronic communications. Relying merely on a single article in the Charter - at the EU level - is insufficient. In the current legal framework the ePrivacy Directive is the instrument of EU secondary legislation that lays down the necessary, specific legal requirements (on the relationship between the GDPR and the future instrument for ePrivacy, see Section III.2 below).

The recognition of confidentiality of communications as a fundamental right in the Charter is in line with European constitutional traditions: the majority of EU Member States also recognise confidentiality of communications as a distinct constitutional right[11] and usually have a distinct body of national law regulating this area. Given the existence of national rules, new more harmonised provisions at EU level contribute to greater legal certainty. As such, they benefit individuals, who are provided equal protection across Europe, as well as businesses, especially those operating in multiple jurisdictions.

II.2 Current level of protection should not be reduced

In addition, we also need new provisions for ePrivacy to maintain the current, higher level of protection for personal data in those instances where the ePrivacy Directive provides more specific safeguards than those foreseen in the GDPR.

For example, whereas the GDPR does not specifically regulate which one of the possible legal grounds for processing may be permitted in which situations, the ePrivacy Directive is more precise in some specific contexts by requiring consent as a legal basis. As an example, Article 5(3) of the ePrivacy Directive requires consent in case of storing or gaining access to information stored on terminal equipment (the so-called 'cookie-rule'). Further, Article 6(3) requires consent for the use of traffic data for marketing purposes or for the provision of value added services. In addition, Article 13 on unsolicited communications also requires prior consent to be the legal basis for certain types of communications under certain conditions.

Further, the ePrivacy Directive also protects legal entities with regard to unsolicited communications as well as in other aspects in their role as subscribers of electronic communications services. The GDPR does not cover these needs[12].

II.3 Precise rules for certain circumstances

The ePrivacy Directive provides rules for a number of situations in which the assessment whether the processing of personal data is involved, who is the controller or processor, and who would be the data subjects could be extremely complex. This concerns, inter alia, technical circumstances related to some network operations (e.g. caller identification), the integrity of the users' end points (information on user terminals) and use of communications services for promotional purposes.

In principle, the ePrivacy Directive addresses such situations without requiring analysis under the conditions of the GDPR. However, the provisions of the ePrivacy Directive itself have been subject to diversity in interpretation. The new instrument should therefore be an opportunity to clarify certain terms or concepts.

III. ISSUES RELATED TO THE LEGAL BASIS

III.1 The legal basis of the new legal instrument for ePrivacy

The EDPS recommends that the Commission consider a dual legal basis for the new legal instrument for ePrivacy. One of these should be Article 16 of the Treaty on the Functioning of the European Union (TFEU). This is the same legal basis as that of the GDPR. The other legal basis should be the current legal basis of the ePrivacy Directive: Article 114 TFEU on approximation of laws (ex Article 95 TEC).

A single legal basis, Article 16 TFEU would be insufficient, as the new provisions will not only 'particularise' some provisions of the GDPR, but will also 'complement' it with provisions that are not limited to the protection of personal data (See also Section II on the *Need for a new legal instrument for ePrivacy* and Section III.2 on the *Relationship between the GDPR and the new legal instrument for ePrivacy*).

III.2 Relationship between the GDPR and the new provisions for ePrivacy

The EDPS recommends that the relationship between the GDPR and the new provisions for ePrivacy remain complementary as it is currently. The current language: '*complements and particularises'* is satisfactory to define this relationship. As a further clarification, we recommend clarifying in a recital that the new provisions for ePrivacy are 'without prejudice' to the current provisions of the GDPR. In other words: the new provisions for ePrivacy should not create additional exceptions from GDPR rules.

We also note that the GDPR concerns the protection of personal data, which is a separate right, set forth in a different article, Article 8 of the Charter. Further, the legal basis of the two instruments (see Section III.1) is also not identical. Finally, the scope of the protected persons is different, as the ePrivacy Directive also provides protection for legal persons.

Whereas it might have been possible to include many provisions of the ePrivacy Directive in the GDPR itself, this has not been the case. Recital 173 and Article 95 call for a clarification of the relationship between the two legal instruments in the new legislative instrument for ePrivacy.

III.3 The choice of a regulation versus a directive

Although the objectives of the review can possibly also be achieved via a directive, the EDPS recommends that the legislators choose provisions in a regulation, rather than a directive as the form of the new legal instrument. This would have the following advantages:

- It would be more consistent with the approach taken in the GDPR;
- It would ensure a more consistent and equal level of protection for individuals and other entities protected by its provisions;
- Further, it would help ensure a level playing field for organisations that need to comply with its provisions, and reduce their compliance costs;
- Finally, a regulation would be better suited to take advantage of the one-stop-shop mechanism, as well as cooperation and consistency mechanisms offered by the GDPR.

That said, it cannot be excluded that there may be some situations where it is necessary to provide some margin of manoeuvre for Member States. This can be achieved irrespective of the type of legal instrument chosen.

We recommend that any such possibilities for diverging national legislation be kept to the minimum necessary. Finally, we recommend that the new legal instrument make a clear reference to the fact that any such national rules, in particular, any exceptions (such as those in current Article 15) must fully respect the provisions of the Charter.

Choosing a regulation would also make it easier to use for ePrivacy the new framework for data protection created by the GDPR with its strong and effective toolkit (e.g. in terms of definitions, scoping and supervision mechanisms), ensuring legal certainty and consistency. The definitions of the GDPR, its territorial scope, the mechanisms for cooperation between enforcement authorities and for consistency, as well as the possibility to provide flexibility and guidance, should be available for ePrivacy.

In its fullest form, this objective could be achieved by selectively integrating as many of the new provisions as possible into the GDPR, if this were conceivable without re-opening the balance of interests made there by the legislators. In this case, the new provisions on ePrivacy could offer controllers and individuals a more simplified and horizontal framework on privacy and data protection within the same GDPR. Even if this option would not be available, the new provisions should ensure that the GDPR framework can be fully used for the new ePrivacy provisions. In any case, we recommend the Commission to consider the option to separate them from non privacy/data protection related provisions for electronic communications.

As the specific legal base may require a new legal instrument, the instrument including the new provisions of ePrivacy should refer to the GDPR and align with it in particular with respect to its definitions, scope with regard to legal persons, data other than personal data (metadata; security; etc.), and all elements supporting enforcement.

In any event, we recommend the legislator to focus selectively only on provisions which appear to be necessary, to then benefit from the provisions in the GDPR allowing DPAs to issue guidance to deal flexibly with the development of new technologies, via the mechanisms the GDPR opens to the EDPB, e.g. on codes of conduct and certifications.

III.4 The relationship with the framework for electronic communications

In its public consultation documents, the Commission does not clearly indicate any position regarding the future relationship of a REFIT ePrivacy instrument with the legislative framework for electronic communications. At present, the ePrivacy Directive is one of the Specific Directives as defined in the Framework Directive[13]. This means that, for example, definitions of the Framework Directive are used in the ePrivacy Directive and need to be interpreted in a consistent and coherent way for the entire framework, i.e. for privacy as well as for radio spectrum administration and economic regulation.

The Commission's decision to launch procedures concerning the ePrivacy Directive apparently without including them in a review of the entire framework indicates that the future provisions on ePrivacy would no longer be an integral part of the legislative framework for electronic communications. The EDPS would welcome such an approach which could help to overcome issues of the current legislation. In particular, in such a scenario the scope and definitions could be defined in function of the specific objectives of the future ePrivacy provisions, without the need to reconcile them with the needs of economic regulation. Moreover, it would become

easier to address the potential overlap of responsibilities between data protection supervisory authorities and other authorities responsible for the supervision and enforcement of electronic communications (see also Section VII below on *Supervision and enforcement*).

IV. THE SCOPE OF THE NEW LEGAL INSTRUMENT FOR ePRIVACY

Historically, rights to the confidentiality of communications have first evolved from the right to the confidentiality of messages sent or received by post. To reflect technological developments, these constitutional rights were in time extended to other means of communications, such as telegraph and traditional telephony. Considering further technological developments, including the rise of communications via providers of so-called over-the-top (OTT) services[14], it is time for the protection to be extended again.

There is a need to update the rules so that they cover new ways of providing communications services. Merely maintaining currently available protection would empty these rights of their substance for an increasingly large portion of our everyday communications.

The challenge lies in ensuring that any new provisions will remain sufficiently technologically neutral to allow coverage of new services, while at the same time affording legal certainty and predictability. Further, extension of scope must be done in such a way that it ensures a high level of protection for users, while at the same time also provides a more level playing field for the organisations concerned.

Finally, the new provisions for ePrivacy must ensure that it is clear and unambiguous as to which organisations must comply with which of their specific requirements. This also calls for a re-thinking of the definitions. The definitions used in the current ePrivacy Directive are designed for general purposes of economic regulation in the telecoms sector and are not targeted specifically at protecting privacy. The meaning of 'public electronic communications network' and 'electronic communications services' is not sufficiently clear and does not reflect today's technological realities. These definitions do not take into account the tendencies of convergence: the blurring of the roles of network providers, virtual network operators and providers of OTT communication services such as internet voice and chat providers. This continues to provide uncertainty to regulators and business organisations alike[15].

IV.1 Instant messaging and voice over IP

From the perspective of the user, there is a functional equivalence between means of communication such as traditional fix-line or mobile telephone and messaging (SMS, MMS) services on one hand and OTT communications services such as Voice over IP (VoIP[16]) and instant messaging apps on the other hand. Individuals must be afforded the same level of protection for all functionally equivalent services, irrespective whether they are provided by traditional telephone companies, by Voice over IP services or via mobile phone messaging apps.

In light of the above, the scope of the ePrivacy Directive could be extended to cover at least those services, which are dedicated to provide functionally equivalent services to traditional electronic communications services for audio, video and text communication (e.g. Voice over IP and instant messaging providers such as Skype, Viber, FaceTime, WhatsApp, Signal, Threema, iMessage or Facebook messenger).

However, in order for the new provisions for ePrivacy to genuinely stand the test of time and provide a technologically neutral framework with a comprehensive level of protection, there is a need to go further: protect not only communications that are 'functionally equivalent' with what traditional telecommunications service providers offer, but also those services that offer new opportunities for communication, possibly as an addition to other offerings.

We also recommend that the Commission carefully evaluate whether there is a need and possibility to cover an even broader range of services. For example, it should be carefully assessed whether communications functionalities integrated into other services (e.g. messaging functionalities in gaming, dating apps) should also benefit of the same or similar protection. The argument for the extension of the protection is based on the fact that user's expectations are often similar with regard to the privacy and confidentiality of these messages and any breach of confidentiality may be equally intrusive. For users, it is possible to begin a conversation using the messaging function of a game, then move to an OTT instant messaging service, exchange mobile SMS' and eventually launch a call between two phones. All these different types of communications may be performed by using the same devices, i.e. smartphones, and for the user different legal frameworks for the services used are by no means evident or even understandable.

IV.2 Internet of Things

The ePrivacy Directive applies to services '*in public communications networks ... including public communications networks supporting data collection and identification devices*' (Art.3). This provision clarifies that the purpose and content of a communication must not affect its protection under the right to privacy. It ensures that the protection of communications privacy is not dependent on whether humans speak or listen, type or read the content of a communication, but that they may rely on the increasingly smart features of their terminal devices to communicate content on their behalf, enjoying the expected level of protection. The communications provider normally should not be concerned with the purpose or content of communications, nor should it even be aware of such specificities of the messages and other communications being transmitted through their services.

While we call it the Internet of Things, in reality it is mostly an 'Internet of Things which are connected to people': IoT contains sports trackers, health sensors, personal communications devices, smart TVs watching their users, intelligent cars tracking every move of their passengers and many other devices. They are equipped with sensors for sound, video, movement and physical parameters of their owners. The fact that they launch their data transfers and communications without the owner triggering it (or even being aware) cannot be a reason to give lower protection to such often sensitive communications.

From the point of view of a communications provider who is subject to the ePrivacy instrument, the content or purpose of a communication cannot play a role for the treatment of its confidentiality and security. The provider should not be concerned whether the message transmitted is the reading of a heart rate monitor or a stock exchange transaction order from a smart trading application, or a photo of a flower bouquet accompanying a wedding invitation. Effective and efficient service, respect for privacy and security must be ensured accordingly for all communications.

The EDPS recommends that the new provisions for ePrivacy unambiguously continue to cover machine-to-machine communications in the context of the Internet of Things, irrespective of the type of network or communication service used. Confidentiality and security of any

electronic communications to and from an IoT device (terminal equipment) should be covered, on all networks and services within the scope. This applies to all relevant provisions, in particular to the confidentiality obligations set forth in Article 5, but also to Articles 6 and 9 covering traffic data and location data.

IV.3 Covering networks of different types

The ePrivacy Directive determines its scope using definitions from the Framework Directive[17]. These definitions have been designed to cover a multitude of purposes including market regulation, spectrum management, universal access, etc. In this complex field, general definitions can only cover the intersection of all fields of application and cannot be tailored to the specific needs of privacy protection. Furthermore, the terminology used in these definitions has often been misunderstood. For example, there are still authors that incorrectly interpret 'public networks' as 'publicly owned', as the term is sometimes used in other contexts.

For independent ePrivacy provisions, it is no longer necessary to ensure that their scope is equivalent to an instrument enabling market regulation. We recommend that the new provisions for ePrivacy also ensure that – in principle - users benefit from the same protection on all networks that they can access. We recommend an expansion that would bring at least all publicly accessible networks and services (including those provided without any commercial interest) within the scope of the confidentiality requirements. These would cover, for example, Wi-Fi services in hotels, restaurants, coffee shops, shops, trains, airports and networks offered by hospitals, universities to the users of their main services (patients or students respectively), as well as corporate Wi-Fi access offered to visitors and guests, and hotspots created by public administrations.

The EDPS further recommends that the new legal instrument for ePrivacy also clarify what should be considered as 'publicly accessible'. For example, it should be made clear that a service remains considered publicly accessible even if the provider limits the service to registered users such as in the case of an organisation offering Wi-Fi access to its customers and visitors.

These comments are following up on previous comments made by the EDPS on the subject. In particular, on the occasion of the last, 2009 review of the ePrivacy Directive, the EDPS issued two Opinions at two different stages of the legislative procedure. In his first Opinion[18], the EDPS argued that '*the rising importance of the mixed (private/public) and private networks in everyday life, with the risk to personal data and privacy increasing accordingly, justifies the need to apply to such services the same set of rules that apply to public electronic communication services. To this end, the EDPS considers that the Directive should be amended to broaden its scope to include such type of private services'.*

In his second Opinion[19], issued at a later stage when specific amendments were discussed during the legislative procedure, the EDPS suggested including under the scope of application of the ePrivacy Directive at least '*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).

V. PROTECTING CONFIDENTIALITY OF COMMUNICATIONS

Protecting the confidentiality of communications (Article 5) must remain a key objective of the new legal instrument for ePrivacy. The EDPS reiterates the central importance of the right to

confidentiality of communications, implementing Article 7 of the Charter. We further emphasize the importance of protecting communications both in transit and at rest. We also underline that new technical paradigms (e.g. cloud computing) further increase the importance of confidentiality[20].

Also, we call attention to the fact that the distinction between content and 'traffic data' is not clear-cut in a multiple service environment as the Internet, where the service provided to the user often combines different technological components in such a way that what, for one component, is considered content constitutes traffic data for another[21].

The processing of data about the communication (such as URLs of websites accessed, e-mail header, traffic and location data) are often equally or even more revealing than the actual contents of the communication.

This has been shown in many examples. For instance, metadata allow for the identification of targets in military drone operations[22]. Metadata can also identify structures in political attacks and criminal investigations[23]. Research has also shown that individuals can be identified from a very limited set of mobile phone location data[24]. It has also been shown that intimate details about a person's lifestyle and beliefs, such as political leanings and associations, medical issues, sexual orientation, habits of religious worship, and even marital infidelities can be discovered through mobile phone traffic data[25].

The new legal instrument for ePrivacy therefore must clearly provide for protection of the confidentiality of communications of both 'content' and 'metadata' (including traffic data and location data).

V.1 Article 5(1): protecting communications while in transit

The EDPS recommends that the new legal instrument for ePrivacy should maintain the general prohibition of interception/surveillance of communications, clearly and specifically covering both content and 'metadata' (including traffic data). We also recommend extending the scope of this prohibition, as suggested above.

Further, to ensure legal certainty, the EDPS recommends that the new provisions for ePrivacy clarify the existing definitions of 'communication', 'traffic data' and 'location data'. This should be done in the main body of the legal instrument for ePrivacy, complemented by a list of examples for each definition in recitals. The provisions, for example, should specify whether a full URL (specifying the visited webpage) is considered content data or traffic data. They should also more clearly specify that the notion of communication does not only include electronic communication between two individuals but also any communications within a defined group (e.g. a conference call, or messages sent to a defined group of recipients).

The EDPS also recommends that the future provisions should specify that interception and surveillance must be interpreted in the broadest technological meaning, including the addition of unique identifiers in the communication such as, for example, advertising identifiers, audio beacons or super cookies.

V.2 Article 5(3): protecting the terminal equipment

The EDPS recommends maintaining and strengthening the consent requirement in current Article 5(3). He also recalls that consent under Article 5(3) will have to be defined and interpreted the same way as under the GDPR.

Article 5(3) protects the integrity of the users' devices against all kinds of unauthorised manipulations and attacks. It is one of the most specific cybersecurity rules in EU legislation. When the user terminal is not protected against interference, the content of communications is only protected on the network, but it could be intercepted, altered or destroyed by malicious interaction with the user terminal before sending or after arriving at its destination: text or data transmissions could be read or modified on the mobile, passwords and PINs could be stolen from the user devices, built-in cameras and microphones could be turned into spying tools. Article 5(3) provides legal protection against such manipulation and misuse, and at least an equivalent level of protection will be needed in the future, as user devices contain more and more important data and critical credentials. In this respect the EDPS recalls his Opinion 8/2015 of 15 December 2015 on the Dissemination and use of intrusive surveillance technologies in which we pointed out that *'the effective protection of ICT systems from any attacks or illicit interception is essential to protect the fundamental rights to privacy and to data protection of individuals in the EU*'.

At the same time, users should be given real control on the use of cookies and similar tools. This includes in particular the choice of device and its features, its further enhancements with additional components and software and the configuration of any features that concern the operation of the device. Recital 66 of Directive 2009/136/EC[26] (Users' Rights Directive) already recognizes the right of the user to control the privacy behaviour of their device through technical features. In an environment where the development of attacks and exploits has the dimension of an industry it is unacceptable to restrict the users' rights to choose technical features protecting their device against interference by third parties. This must also include the right to choose which elements of third party content are executed and block the others, for example scripts that launch interactions between the user device and ad-exchanges or other similar servers.

Consent must be freely given

While the EDPS recommends maintaining the current consent requirement, he also acknowledges that Article 5(3) as currently applied, has failed to live up to its potential to provide a genuine opportunity to choose, and give back control to the individuals. Instead, consent mechanisms have been developed by businesses and other organisations with the objective of arguably meeting the bare legal requirements for compliance under the ePrivacy Directive but failing to give users a genuine choice regarding what is happening to their data. This phenomenon is sometimes referred to as the issue of 'cookie-walls'. Cookie walls, in effect, mean that users who do not accept cookies will be denied access to the websites that they are seeking to access[27]. Many of these cookies continuously track users as they leave their digital trail over the internet, and companies having access to them further use the information obtained for profiling, advertisement and other commercial purposes. This purportedly 'consent-based' and generalised tracking carries high privacy risks and takes control over their personal data completely out of the hands of the individuals concerned.

Cookie walls undermine the idea that consent must be freely given, a key requirement both under Directive 95/46/EC and the GDPR. An improvement compared to Directive 95/46/EC,

the GDPR not only clearly requires that consent be freely given, it now also provides further guidance as to what this means. It provides, among others, that consent is not considered to be freely given in situations where the provision of a service is made dependent on the individual giving his consent to the processing of his personal data despite the fact that the processing of data is not necessary for the performance of such service[28]. This is precisely the case of cookie walls, which often oblige the user to consent to the use of third-party tracking cookies, which are not necessary to the performance of the service concerned.

Considering the importance of a freely given consent, and the often insufficient implementation of Article 5(3) by operators of websites, the EDPS recommends that legislators consider a complete or at least a partial ban on the so-called 'cookie walls'.

In case of a complete ban on cookie walls, the new provisions on ePrivacy should provide that no one shall be denied access to any information society services (whether these services are remunerated or not) on grounds that he or she has not given his or her consent under Article 5(3). This approach would ensure the highest level of protection for individuals, as well as legal certainty and a level playing field for all market players.

As an alternative, in case of a partial ban, legislators could focus their attention addressing at least the most egregious situations, where the impact on users is the highest, or where they have the least amount of freedom of choice. In this case, the new legal instrument for ePrivacy could provide a non-exhaustive list of situations where a choice will not be considered as freely given. At the same time, the new legal instrument for ePrivacy could allow the European Data Protection Board (EDPB) to provide further guidance and specify additional situations where cookie walls are prohibited. The value of this approach lies in its flexibility, but it may offer a lower level of protection for individuals, less legal certainty, and a less level playing field.

In case of a partial ban, the EDPS recommends that at least the following situations should be included on the non-exhaustive list set forth in the new provisions for ePrivacy:

- Situations where the provider of the service is in a dominant position with regard to the services sought by the user;
- all other situations when there is an imbalance of power between the user and the service provider (details to be further elaborated, as necessary, by the EDPB);
- communications and services fully or partially funded by taxpayers' money (e.g. websites offering e-government services; news media supported by government subsidies or compulsory license fees);
- any situations in which special categories of data could be inferred from the data collected, in itself or in combination with other data (e.g. visits to news websites or websites offering health information, online bookstores, use of fitness apps, tracking location data in a place of worship or a hospital);
- situations where a website or app auctions its advertising space and unknown third parties may track and monitor users through the website or app;
- bundled consent for multiple purposes (e.g. where consent for marketing and for value added services cannot be given/withheld separately).

In case the ban is only partial, the EDPS recommends that the new provisions for ePrivacy further provide that irrespective of the market power of the service provider, it must (i) either

provide a choice whether or not to provide consent to processing data not necessary for the provision of the service without any detriment, (ii) or at least, make available a paying service at a reasonable price (without behavioural advertising and collection of data), as an alternative to the services paid by users' personal information. This possibility has already been referred to by the Commission in its public consultation[29].

Mechanisms for providing and revoking consent

Finally, the EDPS emphasizes that users must have user-friendly and effective mechanisms to provide and revoke their consent. The EDPS recommends, building on recital 66 of the Users' Rights Directive referred above, that the new provisions for ePrivacy provide for a workable legislative requirement ensuring that the user's consent to the processing could be expressed by using the appropriate settings of a browser or another application.

This means that instead of merely relying on website operators to obtain consent on behalf of third parties (such as advertising and social networks), the new legal instrument for ePrivacy can require that browsers and other software or operating systems offer 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 their consent or lack thereof.

Such tools must be offered to the user at the initial set-up with privacy-friendly default settings.

Adherence to accepted technical and policy compliance standards by all parties concerned, including the operators of the website, should become obligatory.

Need for a technologically neutral and more inclusive wording

Further, the current wording of Article 5(3): '*the storing of information*', or the '*gaining of access to information already stored*' in the terminal equipment of users, has left some margin for diverging interpretations as to which types of interaction of a third party with the user device are covered, in particular regarding what constitutes 'g*aining access to information already stored*'. While it is clear that any unauthorised interference with the device should be covered, there are less clear-cut cases. Should the collection and use of information that the user device provides by default as part of standard communications behaviour be considered as gaining access to information already stored? If the information is not provided by default, should an information request that is supported by the communications protocol used between terminal and third party be considered as gaining access? Should information that is only produced in response to a request from the third party (e.g. battery level measured in reaction to the request) be considered as information already stored? How should information be considered that is associated to the user terminal and accessible through it, but not stored on it physically, and loaded from a cloud service in order to respond to the request from the third party?

The EDPS considers that in the light of the examples listed above, the technical implementation should not be the criterion to determine the level of privacy protection of the user, even more so as in some cases neither the user nor the third party requesting information may be aware of the exact technical circumstances of an information request. Therefore, the wording of the instrument should be as technologically neutral and inclusive as possible. For example, it should be ensured that all current and future tracking techniques used via smartphones and in IoT applications are fully covered. The rules, in particular, should cover device fingerprinting, as well as all forms of 'passive tracking', that is, the use of identifiers and other data broadcasted

by devices. With the development of the Internet of Things, more and more data will likely to be broadcast 'by default'. Rather than considering the condition that information is 'already stored, in the terminal equipment', the condition could cover all information that can be obtained from the device. Such operations would require consent with the exceptions for transmission and provision of a service, as currently laid down, with a possible extension for a very limited case of processing directly related to a service requested by the user and performed exclusively by the service provider.

Exception for first-party analytics cookies

Further, while clarifying the scope of the consent requirement, the new legal instrument for ePrivacy should also create an additional exception for first party analytics cookies, subject to adequate safeguards[30]. This should help ensure that data can be processed when this causes little or no impact on the rights of users to the confidentiality of their communications and private life. The EDPS recommends that any such exceptions be limited to cases where the use of such first party analytics cookies is strictly limited to aggregated statistical purposes. In addition, adequate safeguards must be applied including clear information provided to the individuals concerned, a user-friendly mechanism to opt out from any data processing, and appropriate anonymisation techniques applied to collected information such as IP addresses. The Article 29 Data Protection Working Party in its Opinion 04/2012 on Cookie consent exemption[31] already called legislators to create such an exception.

For more guidance on the safeguards to be applied and the conditions under which a first party analytics cookie can be exempted from the consent requirement, the new legal instrument for ePrivacy may refer to future guidance to be provided by the EDPB.

V.3 Traffic data and location data

Metadata about communications can provide a very detailed profile of an individual and processing it can be just as intrusive as processing 'content' of communications.

These data are no longer only collected by traditional telephony and internet service providers. A range of new service providers may also obtain a very detailed overview of a users' travel and communication patterns, social networks, and others. At the same time these service providers are currently not subject to the obligations of the ePrivacy Directive.

By requiring consent for the processing of traffic and location data, the current ePrivacy Directive offers a higher level of protection than the GDPR. The GDPR, at least potentially, allows other legal grounds, such as legitimate interests or performance of a contract. A controller might try to argue, for example, that tracking users over the internet, and building detailed profiles for them would be part of their legitimate interest to market their services and products.

In order to better protect the confidentiality of electronic communications, the EDPS recommends that the ePrivacy Directive maintains and strengthens the current consent requirement for traffic and location data. In particular, he recommends that the ePrivacy Directive be revised to include a single consent requirement for the processing of metadata. This should apply to all traffic and location data, irrespective of who collects and processes such data. In other words: the scope of this provision, similarly to Article 5(3), should be broadened to cover everyone and not just traditional telephone companies and internet service providers.

VI. PROTECTING SECURITY OF COMMUNICATIONS

It is essential that the current level of protection be maintained: legislators should not create a regulatory gap by removing the existing security obligations in the ePrivacy Directive.

The security requirements in the GDPR only apply to cases where personal data is concerned. However, there is a need to ensure that other data, e.g. confidential business information, that does not always necessary also contain personal data, remain protected. Other legal instruments, such as the so-called NIS Directive[32], also only provide coverage for certain situations.

Therefore, there remains a need for specific provisions on security also in the new legal framework for ePrivacy[33].

Further, there should be no ambiguity about the scope of any requirements to protect the security of communications: the new provisions for ePrivacy should clearly provide (in the main body of the text, not only in a recital) for the confidentiality and security of communications while in transit but must also protect the confidentiality and security of end user equipment. The EDPS recommends that Article 4 of the ePrivacy Directive should be revised to clearly cover both situations. The new provisions for ePrivacy should also ensure that Article 5(3) or a similar provision continue to protect end user equipment against spyware.

VI.1 The need for additional measures on security in the new provisions for ePrivacy

The EDPS also considers that the following additional security measures mentioned in the public consultation of the Commission[34] would be necessary:

- development of minimum security or privacy standards for networks and services;
- extending 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;
- extending security requirements to reinforce coverage of IoT devices, such as those used in wearable computing, home automation, vehicle to vehicle communication, etc; 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.

These requirements could assist in the proper implementation of principles of security by design, data protection by design and data protection by default, and would provide more guidance for manufacturers and software providers.

Standards can extend security requirements so as to ensure coverage of network providers, providers of network components, terminal (including IoT) or complementary equipment (including software) used in combination with the provision of electronic communications services.

VI.2 Encryption

As it has also been pointed out by the WP29, *'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 organisations and governments to gain access to communications'*[35].

The EDPS recommends that the new provisions for ePrivacy clearly allow users to use end-to-end encryption (without 'back-doors'[36]) to protect their electronic communications. The EDPS further recommends, as also suggested by the WP29, that decryption, reverse engineering or monitoring of communications protected by encryption should be prohibited.

In addition, the use of end-to-end encryption should also be encouraged and when necessary, mandated, in accordance with the principle of data protection by design. In this context the EDPS also recommends that the Commission consider measures to encourage development of technical standards on encryption, also in support of the revised security requirements in the GDPR.

The EDPS further recommends that the new legal instrument for ePrivacy specifically prohibit encryption providers, communications service providers and all other organisations (at all levels of the supply chain) from allowing or facilitating 'back-doors'.

VI.3 Data breaches

The EDPS recommends deleting Articles 4.3 and 4.4 of the ePrivacy Directive on data breaches as the GDPR already requires all controllers to notify subscribers and competent national authorities of personal data breaches (subject to certain exemptions). To avoid duplicate notifications we recommend that all data breaches involving personal data should be notified to the supervisory authorities provided for in GDPR according to the provisions set forth therein.

VII. SUPERVISION AND ENFORCEMENT

Under the current ePrivacy Directive, there are a number of different authorities that are responsible for the supervision and enforcement of the various provisions of the Directive. Experience has shown significant variations across Europe and also overlaps or duplications between the roles of the various supervisory authorities[37]. There is therefore a need to simplify the existing framework.

In addition, it must also be kept in mind that the GDPR creates new obligations for the supervisory authorities, such as cooperation between competent national authorities, the consistency mechanism and the role of the EDPB. If supervision of (parts of) the new legal instrument for ePrivacy were to be performed by an authority, which is not a data protection authority, an effective mechanism must be designed for such an authority to be represented in the cooperation mechanisms of the data protection authorities. This could add additional complexity to an already complex arrangement for cooperation.

In light of these considerations, in all cases where a task can be effectively carried out by a national data protection authority, for the sake of legal certainty and ease of practical implementation, we recommend considering the national data protection authorities as the competent authorities.

VIII. UNSOLICITED COMMUNICATIONS

The EDPS recommends that the current rules in the ePrivacy Directive protecting against unsolicited communications be maintained, updated and strengthened during the review. The means by which unsolicited communications are conducted have evolved since the ePrivacy Directive first came into force. As an example, an unsolicited voice call can start with an automated dialler, 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, the EDPS recommends that the new provisions for ePrivacy adopts a technology neutral approach. Article 13 should require the prior consent of recipients for all types of unsolicited electronic communications, independent of the means (e.g. electronic mail, voice or video calls, fax, text, but also direct-messaging (i.e. within an information society service) and behavioural advertisement. Further, the level of protection should be equivalent, irrespective whether the user/subscriber is a natural person or a legal entity.

Current exceptions regarding existing relationships and similar products and services should be preserved but we recommend that the new provisions for ePrivacy clarify what is meant by existing relationship and similar products and services.

The current ePrivacy Directive focuses on 'commercial' communications. Yet not all spam and malicious communications can be considered commercial in any usual business sense. Strictly speaking, communications related to crime attempts, e.g. phishing attacks and fraudulent financial proposals may not always be covered by this qualification. It is recommended that the legislator verify possibilities to provide a more comprehensive definition to cover all types of spam, unsolicited telephone calls and marketing messages, phishing and other malicious attempts.

IX. DIRECTORIES OF SUBSCRIBERS

Article 12 of the ePrivacy Directive provides for the right to subscribers to '*determine whether their personal data are included in a public (printed or electronic) directory.*'

The EDPS recommends maintaining this provision and extending its scope to include all kinds of directory services. Further, the consent requirement for 'reverse lookup' should also be explicitly extended to other service identifiers such as email address or user name.

X. ADDITIONAL RECOMMENDATIONS

X.1 Calling line identification (CLI)

The ePrivacy Directive includes a right for call recipients to be informed about who is calling them and take action against those calls, which withhold their CLI. The EDPS recommends maintaining this right, as one of the protections enabling individuals to take action against those engaging in unsolicited communication in violation of applicable law.

X.2 Territorial scope and applicable law

The EDPS recommends that in principle the new provisions for ePrivacy have unambiguously the same territorial scope compared with the GDPR (including the extra-territorial scope provided for in Article 3(2)[38]) and follow in principle the same approach in terms of applicable law about personal data processing.

At the same time, it must be considered that there may be a need for some technical adjustments in the wording of these provisions. For example, Article 5(3) of the ePrivacy Directive applies whether or not the person who set a cookie or deployed a spyware is considered as a 'controller' under the GDPR, and whether any personal data is processed. Therefore, the territorial scope may also need to reflect these differences.

X.3 Transparency regarding government access requests

In global networks, communications cross borders without the users being aware. On the one hand, communications between EU Member States may pass through third countries; on the other hand, communications between third countries may be transmitted via EU territory. Communications service providers established or operating in the EU may be subject to requests for information or access to their users' data from law enforcement or security services of other Member States and non-EU countries, based on the applicable national laws and practices creating exceptions to the right to confidentiality of communications. Following the entry into force of the GDPR, such requests requiring personal data to be transferred to a third country will only be based on an international agreement, such as a mutual legal assistance treaty[39].

The use of security and law enforcement powers to breach the confidentiality of communications must be in line with the principles of necessity and proportionality. While informing the individuals subject to such measures may be restricted for instance in order to safeguard the objectives of an ongoing investigation, a general awareness about the frequency and volume of disclosure requests addressed to communications service providers would give citizens in general and also public bodies the possibility to benchmark and assess the general practice in the use of these instruments. Transparency regarding government access requests may thus play an important role in helping ensure respect for fundamental rights.

Therefore, the EDPS recommends that the new provisions for ePrivacy provide specific rules enhancing transparency. In particular, he recommends a new provision creating an obligation for organisations to disclose, at least periodically and in an aggregate form, law enforcement and other government requests for information. This should cover requests from both inside and outside the EU. With regard to such requests from third countries, the service providers should observe the legality condition provided for in Article 48 of the GDPR.

XI. CONCLUSIONS

The importance of confidentiality of communications as laid down in Article 7 of the Charter is growing with the increased role that electronic communications play in our society and economy. The safeguards outlined in this Opinion will play a key role in ensuring the success of the Commission's long term strategic objectives outlined in its DSM Strategy.

Done in Brussels,

(**signed**)

Giovanni BUTTARELLI

European Data Protection Supervisor

Notes

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p.37; amended by Directive 2009/136/EC.
[2] Ref. Ares(2016)2310042 - 18/05/2016.
[3] See https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive. The questionnaire is available at: https://ec.europa.eu/eusurvey/runner/EPRIVACYReview2016.
[4] WP29 Opinion 3/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC) (WP240) adopted on 19 July 2016.
[5] A Digital Single Market Strategy for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, 6 May 2015 (COM(2015) 192 final) available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN.
[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); OJ L 119, 04.05.2016, p.1, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL
[8] See endnote 4.
[9] See https://edri.org/files/epd-revision/EDRi_ePrivacyDir-final.pdf.
[10] Article 7 of the Charter also protects the right to privacy.
[11] See, for example, Article 10 of the German Constitution, Article 37 of the Slovenian Constitution, Article 36 of the Croatian Constitution, Article 19 of the Greek Constitution, Article 43 of the Estonian Constitution, Article 15 of the Italian Constitution, Article 49 of the Polish Constitution, Article 28 of the Romanian Constitution, Article 72 of the Danish Constitution, Article 13 of the Dutch Constitution, Article 29 of the Belgian Constitution, Article 6 of Chapter 2 of the Swedish Constitution, Article 10 of the Finnish Constitution, Article 17 of the Cypriot Constitution, Article 18 of the Spanish Constitution, Articles 10 and 10a of the Austrian Constitution, Article 13 of the Czech Constitution and Article 22 of the Slovak Constitution.
[12] See Article 1 and recital 14 of the GDPR with regard to legal entities, which make it clear that the GDPR grants the right to the protection of personal data only individuals and not legal entities.
[13] 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), as amended.
[14] Over the top (OTT) refers to services and applications that are accessible using the Internet and rely on a network provided to offer Internet access services. Examples include communications (voice and messaging) services such as Skype, WhatsApp and Facebook Messenger, but also a broad range of other services and applications, such as social networks like Facebook, Twitter or LinkedIn, or video and audio streaming services such as Netflix or YouTube. For more on OTTs, see, e.g. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf.
[15] It is also notable that often a user may initiate a voice or text communication via an OTT communications service but the recipient may receive the message or partake in the communication via traditional means (e.g. may receive an SMS on his mobile phone or receive a VOIP call on his traditional fixed line telephone).
[16] Strictly speaking, VoIP is a family of protocols that supports the provision of telephony services over networks using internet protocols (mainly IP) instead of traditional telephony standards. These technologies are used by so-called OTT providers, but also by traditional network providers. In the regulatory context the term 'VoIP' is often used as a synonym for internet telephony provided on top of the basic transmission networks. This is the meaning applied in this Opinion.
[17] See endnote 13.
[18] Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), issued on 10 April 2008 (2008/C 181/01), available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_EN.pdf See in particular, paras 22-24.
[19] Second Opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive

on privacy and electronic communications), issued on 9 January 2009 (2009/C 128/04), available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_EN.pdf See, in particular, paras 60-72, including the quoted text in para 66.

[20] See, e.g. Science and Technology Options Assessment (STOA), European Parliament, *Potential and impacts of cloud computing services and social network websites*, 2014. PE 513.546. Available at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf

[21] For the technological background, please refer to the OSI model https://en.wikipedia.org/wiki/OSI_model and the Internet protocol suite https://en.wikipedia.org/wiki/Internet_protocol_suite.

[22] 'We kill people based on metadata' was a statement made by former CIA and NSA Director Michael Hayden at John Hopkins University in April 2014. See: Pomerantz, J., Metadata, United States of America: MIT Press 2015, p. 118. The speech at John Hopkins University is available at: https://www.youtube.com/watch?v=kV2HDM86XgI with Mr Hayden's quote at 17:59 minutes.

[23] Metadata had been used during the criminal investigation, resulting in the apprehension of the accused assassins of former Prime Minister Rafiq Hariri. *'Of the 10 mobile phones used in connection with these 10 cellular telephone cards, 5 have been traced to a store in Tripoli.*' United Nations Security Council, Report of the International Independent Investigation Commission established pursuant to Security Council resolution 1595 (2005), S2005/662, Beirut: 19 October 2005, nr. 151, p. 147, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/563/67/PDF/N0556367.pdf?OpenElement.

[24] De Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013), *Unique in the Crowd: The privacy bounds of human mobility*, Nature SRep, 3, available at: http://www.nature.com/articles/srep01376 showed that four spatio-temporal points are enough to uniquely identify 95% of the individuals.

[25] New York Times Editorial Board, Surveillance: *A Threat to Democracy*, 11 June 2013, available at: http://www.nytimes.com/2013/06/12/opinion/surveillance-a-threat-to-democracy.html?hp.

[26] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009. p. 11, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.

[27] A similar phenomenon occurs also in the world of mobile apps where the apps often request permission to access different capabilities and functions of a mobile phone, which are not necessary for the functioning of the app and provision of the service, including access to Wi-Fi, GPS, camera, messages, contacts, browsing history or pictures. An example may be torch app whose functionality is to provide a bright flashlight, but which requests overbroad data access to many of the above data categories clearly unnecessary for the functioning of the service it provides.

[28] The GDPR, in its recital 42, emphasizes that *'[c]onsent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment'*. It also highlights that *'a declaration of consent pre- formulated by the controller ... should not contain unfair terms'*. Further, recital 43 provides that *'[i]n order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller.'* Recital 43 also provides that *'consent is presumed not to be freely given ... if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.'* This latter point has also been reiterated in Article 7(1) of the GDPR, which provides that *'[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract'*.

[29] See Question 22 on the Commission public consultation: 'Information society services should be required to make available a paying service (without behavioural advertising), as an alternative to the services paid by users' personal information'.

[30] It should be clear in the legislative text that when an organization uses analytics services from a third party (like Google Analytics), which are setting their own cookies, these cannot be considered as first party cookies.

[31] Opinion 04/2012 of the Article 29 Working Party on the Cookie Consent Exemption (WP194), available at: http://ec.europa.eu/justice/data-protection/article-29/documentationopinion-recommendation/files/2012/wp194_en.pdf.

[32] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p.1.

[33] That said, the GDPR and the new legal instrument for ePrivacy should be aligned to ensure consistency. For example, the EDPS recommends a cross-reference to the security obligations in the GDPR (including data protection impact assessments and accountability).

[34] See question 21 of the public consultation questionnaire.

[35] See WP29 Opinion referenced in endnote 4, p. 19.
[36] See https://en.wikipedia.org/wiki/Backdoor_(computing).
[37] Study on the 'ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation' (SMART 2013/0071), Section 3.2.3 on *Supervision* (pp. 33 and 34). Available at: https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.
[38] See also the joint analysis of civil society groups referred to in endnote 9 above.
[39] See Article 48 GDPR *'Transfers of disclosures not authorised by Union law'*.