DIGITALEUROPE

DIGITALEUROPE views on the Review of the ePrivacy Directive

Brussels, 31 October 2016

EXECUTIVE SUMMARY

DIGITALEUROPE as the voice of Europe's digital technology industry welcomes the opportunity to work closely with the EU Institutions as they review and assess the ePrivacy Directive ("ePD"). Our members are committed to the highest standard of data protection, privacy, security and integrity of the digital ecosystem. However, for Europe to attract and sustain the world's best technology companies that can contribute to a strong digital economy, businesses need a regulatory environment which is not only predictable, but avoids unnecessary burdens and overlaps with existing legislation. As the EU Institutions continue to understand and consider the future role of the ePD, DIGITALEUROPE believes any future actions by policy makers should take into consideration the following:

- The Future of ePrivacy - The priority of the review should be to achieve simplification of the legal framework and consistency with other legal instruments. To the extent that any of the provisions of the ePD are still necessary, these could be integrated into other legal instruments, such as the European Electronic Communications Code.

- Scope – The potential extension of scope to cover OTTs, IoT devices, and M2M communications is not necessary to ensure the appropriate level of protection for consumers.

- Security – The security provisions under the GDPR have the exact same objectives as the ePD. Keeping Article 4 or any version of this provision would only duplicate existing requirements.

- Traffic & Location Data – Maintaining a separate set of rules on traffic and location data and extending it to some new services would considerably increase legal uncertainty, as two sets of regulatory requirements would be now applicable to the exact same data sets.

- Ensuring Confidentiality of Communications – A more focused approach on confidentiality requirements is needed when considering the practical implications on network operators and providers of services who rely on third party connections. If a broad expansion of confidentiality occurs, derogations must be provided to allow for legitimate activities of service providers.

- Confidentiality & Law Enforcement – The right to the confidentiality of communication should not only apply to the commercial context alone. The protection granted by the Charter is universal and should also be ensured in the law enforcement and national security context. Any mandate requiring service providers to reverse engineer, provide back doors and any other measures to weaken their security/encryption measures should be explicitly prohibited.

- Device Data (including "Cookies") – Any suggestions that would seek to prohibit businesses from preventing access to their services if the user refuses to accept a cookie must be avoided. This would not only disproportionately interfere with the freedom to conduct a business and the freedom of contract, but also undercut the EU's competitiveness in the data-driven and knowledge-based digital economy.

- Enforcement – Enforcement powers should be conferred on the public agency that is the most competent in the matter at hand. Issues related to personal data should solely be dealt with by national data protection authorities.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

1. The Future of ePrivacy

The review of the ePD offers a unique opportunity to simplify and streamline legislation in line with the European Commission's Better Regulation Agenda; and to achieve a simple, consistent and meaningful set of rules designed to protect citizens' privacy and personal data.

DIGITALEUROPE agrees with the European Commission that the priority of the review should be to achieve **simplification of the legal framework and consistency with other legal instruments**. We welcome the European Commission's suggestion[1] to consider all options to achieve this, including "*repealing outdated or unnecessary provisions*" as well as "*a total repeal of the Directive*".

This is important as the General Data Protection Regulation ("GDPR") will offer a comprehensive, clear and higher level of protection regarding the processing of all types of personal data including data governed by the current ePD. In fact, part of the European Commission's reasoning behind the GDPR was the need to address "*the rapid pace of technological change and globalization*", and the '*new ways of sharing information through social networks and storing large amounts of data remotely' becoming 'part of life for many European users'*". The new legal framework not only includes separate provisions and safeguards for sensitive data and risky processing (i.e. explicit consent, impact assessments and prior consultation), but also incorporated and expanded ePrivacy provisions on security, breach notification regime, and the processing of location and traffic data.

As we stated in our joint industry statement in July 2016[2], to the extent that any of the provisions of the ePD are still necessary, these could be **integrated into other legal instruments, such as the European Electronic Communications Code ("Draft Code").**

DIGITALEUROPE therefore believes that the GDPR creates the ideal scenario for the European Commission to achieve its stated objective of ensuring that the rules governing the telecommunications sector are "simple, flexible, technology-neutral and aim at deregulation in the longer term".[3]

2. Scope

Our understanding is that the scope of services to be covered by the ePrivacy framework will be largely set by the definition of Electronic Communication Services ("ECS") under the proposed Draft Code.

We are **concerned to see that the current scope of services has been significantly expanded** to also cover online communication services ("interpersonal communication services") and services that merely convey signals (Machine-to-Machine (M2M) or Internet of Things (IoT)). We question the necessity to expand the existing legal framework to cover new online communication services (so-called over the top services or OTTs), as it was precisely these services that the GDPR and the Network and Information Security ("NIS") Directive were designed to capture. **Further extending telecoms regulations to OTTs is not necessary to ensure the appropriate level of protection for consumers.** As we explain in the following section of this paper, all services are subject to a variety of EU legislation that ensures this protection in the digital space, most importantly the GDPR and such legislation already does so in a service and technology neutral manner (i.e. without distinguishing between the different types of communication and other online services).

[1] Inception Impact Assessment – REFIT Evaluation and Impact Assessment of Directive 2002/58/EC (October 2016)
[2] Joint Industry Statement – Empowering trust and innovation by repealing the e-Privacy Directive (July 2016)
[3] https://ec.europa.eu/digital-single-market/en/telecoms-rules

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

Instead, given the already existing and appropriate safeguards achieving the desired protections for consumers and competition, regulators should **repeal the telecoms and other provisions of the ePD**, which are no longer necessary. This is a simple and easy way to achieve a consistent application and enforcement of a single set of data protection principles.

3. Security

Article 4 of the ePD requires that publicly available electronic communication service providers adopt technical and organisational measures to safeguard the security of services appropriate to the risk. This is complementary to Article 13a in the Framework Directive (new Article 40 of the Draft Code) and the NIS Directive insofar as the focus is on security of data processing as opposed to the integrity of the network (and continuity of services) found in the other two instruments.

However, it is important to underline that the **security provisions under the GDPR have the exact same objectives as the ePD**. As the Communication[4] of the European Commission accompanying the release of the GDPR proposal underlines, the security provisions of the Regulation build on the ePD.

Article 4 also makes it clear that the main objective is to protect personal data. As pointed out by others, in accordance with Article 4 (1.a) the measures of the ePD shall at least (i) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes; (ii) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and (iii) ensure the implementation of a security policy with respect to the processing of personal data.

Similarly, breach notification requirements exist under GDPR, NIS and most probably under the new Draft Code.

It is clear that **keeping Article 4 or any version of this provision would only duplicate existing requirements**, leading to legal uncertainty without providing any additional protection whatsoever to the end user. DIGITALEUROPE is thus convinced that the combination of the NIS, Article 40 of the Draft Code and the GDPR provide a high level of protection make any further legal intervention **unnecessary and counterproductive**.

We therefore recommend repealing Article 4.

4. Traffic & Location Data

DIGITALEUROPE would like to underline that during the discussion leading to the adoption of the GDPR, the question of scope was widely debated. As a result, the definition of personal data (Article 4 (1)) now specifically references location data and online identifiers.

However, the European legislator clearly did not consider it necessary to include in the GDPR specific rules on the processing of location data or online identifiers. It simply applied the overall requirements and extended the requirements of a context and risk based approach to these data sets as well.

We would also like to recall that the **GDPR contains important safeguards and makes the principles in Article 5 applicable to all data covered by the scope**. Maintaining a separate set of rules and extending it to some new

[4] COM/2012/09 final - Communication from the European Commission on Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century (January 2012)

services would **considerably increase legal uncertainty, as two sets of regulatory requirements would be now applicable to the exact same data sets.**

Regulating these data beyond the GDPR would also imply that the Regulation is already no longer considered as an appropriate tool to achieve its goal, notably offering a high level of protection in a digital age.

DIGITALEUROPE strongly believes that **rejecting this double regulation would not lead to a decrease of the level of protection offered to users of communications services**. On the contrary, clarity of the rules ensured by relying on the GDPR would benefit both consumers and businesses alike.

We therefore recommend repealing Articles 6 and 9 of the ePD.

5. Ensuring Confidentiality of Communications

DIGITALEUROPE members support the fundamental right to the confidentiality of communications. Our strong stance on Better Regulation and simplification of the legal requirements **does not call this commitment into question** as we strongly believe that the two are perfectly in line.

It seems that the only real reason for maintaining the current ePrivacy framework is to ensure that the fundamental right to private communications (as established in Article 7 of the European Charter of Fundamental Rights) is respected. Arguably a standalone legal instrument, such as the ePD, is not necessary to ensure that communications remain confidential. The **right is fundamental in EU law and there is a wealth of EU national and case law where this right has been enforced and concretely implemented, even outside privacy legislation**.

However, and to the extent that a version of the provisions of Article 5 of the ePD is still deemed necessary, instead of keeping a standalone ePrivacy legislation just for this, the **provision could be integrated into the proposed Draft Code.**

If the provisions of Article 5 should be maintained, it is important to **modernise these in light of technological developments**. A broad expansion of confidentiality requirements could place unnecessary restrictions and create ambiguity over legal liability for both operators of public and private networks and providers of services that are accessed through a user's connection to such networks. We note that today Article 5 only envisions that service providers will process communication for the purposes of transmitting or routing a communication. The reality is that there are a wide-range of legitimate circumstances in which service providers must have access to communications that are processed or stored on their systems.

As correctly pointed out by the Article 29 Working Party, this includes ensuring the protection of networks and information systems. However, we wish to stress that there are other legitimate circumstances where service providers might need to access communications which are stored on their systems. These include but are not limited to:

- **Malware or other threat screening** – Service providers routinely scan communications for malware, phishing and other attacks. Businesses need to be able to continuously scan incoming data packets for cybersecurity threats.
- **SPAM detection** – Service providers use a variety of automated tools to filter communications for spam or other undesired actions. Furthermore, features for searching and archiving stored communications require access to communication content. Businesses need to continue to be able to execute such legitimate activities.

- Filtering out illegal or unacceptable content – Service providers often rely on automated tools to scan communications and files for illegal content, violent and graphic images, and other content that violates user policies and community guidelines. Businesses should be allowed to continue such activities.
- Preventing the loss of data and unauthorised access – Service providers (as well as government agencies) often rely on automated tools to scan communications to prevent data loss and detect unauthorised access to a closed internal network. These systems require the ability to inspect communications travelling within a network as well as those communications seeking to enter and exit a network. Businesses, particularly those that rely on third-party cloud vendors for such monitoring, must be allowed to continue such legitimate activities.
- Product features – Certain product features of service providers provide enhanced capabilities that go far beyond transmitting and routing communications. Product features such as translators, bot functionalities, group video callings, message syncing across devices, or assistive technologies that automatically copy hotel reservations, travel itineraries, etc., in the users' calendar are not possible without access to the communications content itself.
- Anonymisation – Service providers must be able to access communications to execute anonymisation techniques in line with privacy principles. This will help businesses improve their services and increase privacy protection.

Organisations and consumers rely on service providers for many of the capabilities described above in order to secure their data and systems and comply with legal requirements. Service providers must have access to communications that are processed or stored on their systems in order to deliver the services purchased by their customers.

We also strongly believe that no law should restrict an individual's ability to access and use the best possible technology/methods to secure and protect the confidentiality of the communications. Our companies develop and make available many of the tools that ensure that consumers' transactions and communications remain confidential and secure. This is achieved through a variety of solutions, most notably end-to-end encryption. However, our companies **fear than an expansion of the ePD to cover OTT services risks to undermine the very privacy it is seeking to protect**. This concern was reinforced by the recent joint German/French initiative on encryption, which identified the ePrivacy review as a vehicle to address law enforcement frustrations.

We therefore propose that Article 5 should be either repealed or integrated into the proposed Draft Code.

6. Confidentiality & Law Enforcement

The **right to the confidentiality of communication should not only apply to the commercial context alone**. The protection granted by the Charter of Fundamental Rights is universal and **should also be ensured in the law enforcement and national security context**. The definition of ECS forms the basis of national data retention and interception laws. An extension of the scope would thus have an immediate impact on users' privacy.

Whilst we understand the need for law enforcement and national security agencies to access data, subject of course to adequate safeguards and proper legal processes, a seemingly simple extension to cover all online communication services, M2M communications, etc., will in fact achieve an **anti-privacy goal of potentially opening all of these services to national data retention and interception obligations**. Many of these services are engineered to apply the best possible encryption technology to reinforce security and confidentiality of the

communication. They were not designed to comply with many of the data retention and interception obligations, which would in fact have an adverse impact on the security of these services.

Finally, in addition to existing safeguards provided in Article 15 (1) (i.e. that measures need to be necessary, appropriate and proportionate), **DIGITALEUROPE strongly recommends to ensure that any measures cannot result in a weakening of the security and integrity of the service**.

Furthermore, any mandate requiring service providers to reverse engineer, provide back doors and any other measures to weaken their security/encryption measures **should be explicitly prohibited**. Instead, as stated above, provisions should allow and possibly encourage communication services to provide users with solutions that allow them to secure their communication, such as strong encryption.

7. Device Data (including "Cookies")

Article 5(3) of the ePD is often referred to as the "cookies" provision. However, it is important to note that the requirements may be interpreted more broadly as they require consent of the subscriber or user to store or access any information on their terminal equipment.

DIGITALEUROPE does not believe that maintaining Article 5(3) is necessary to achieve the high level protection of consumers privacy, already guaranteed by the GDPR.

After the entry into force of the ePD, it became clear how **counterproductive an overly strict interpretation of the opt–in requirement is, leading to an overexposure of consent requirements and desensitising users**. Therefore, we caution against an over-reliance on consent as experience has shown that people do want a degree of control, but do not want constant consent/permission requests, particularly for activities they do not care about, and which are unlikely to expose them to any harm.

As the study[5] commissioned by the European Commission highlights, the introduction of the consent rule in Article 5 (3) has **not reached its objective**. The "warning fatigue" highlighted by the study occurs because the exemptions contained in Article 5(3) are too narrow. In fact, Article 5(3) requires information and prior consent in all cases, unless such storage or access take place to ensure the communication or otherwise strictly necessary for the provision of an online service requested by the user.

These exceptions have been interpreted very narrowly. For example, it would not be considered 'strictly necessary' for a device manufacturer simply to understand how its own devices has been set up, or for a website designer simply to understand how his/her own website is performing, in a manner that ultimately leads to the production of anonymous, aggregate data that has **no privacy impact**, but is extremely valuable to the manufacturer or website designer for general design improvement and the development of new products and services. While this and similar activities have no privacy or data protection implication, the users' consent may still be required.

Indeed, storage and access are required for various different purposes, such as those i) aimed at maintaining and managing security and integrity; ii) aimed at obtaining information about the quality and/or effectiveness of a provided service; and iii) within the scope of legitimate interest under the GDPR.

[5] ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation (January 2015)

The **GDPR makes these rules redundant** and ensures a risk-based approach that would allow for meaningful notification and control provisions to emerge. The GDPR reflects the already broad interpretation of the definition of personal data under the 95 Directive by, for example, explicitly including online identifiers, such as cookies in the definition. As a result, in all cases where there may be a privacy impact of the storage or access of information on an end-user device, this will involve the processing of personal data.

Article 6 of the GDPR requires that all processing of personal data satisfy one of the legal grounds outlined in the Regulation. Where access to or the storage of data is not necessary for the performance of a contract (Article 6(1) (b)) and would be overridden by the interests or fundamental rights and freedoms of the data subject (Article 6(1) (f)), consent will most certainly be required (Article 6(1)(a)). The **GDPR therefore already provides the balanced and risk based transparency and control requirements that Article 5(3) ought to provide.**

It would allow cookies needed for analytics (aggregated statistics), the functionality of certain features (i.e. shopping basket), security or authentication, etc., but would address concerns about tracking (which our member recognise) and require consent for access and storage that would likely result in a privacy impact for data subjects.

DIGITALEUROPE, therefore, concludes and strongly recommends repealing Article 5(3).

In much the same way, we **oppose any suggestions that would seek to prohibit businesses conditioning access to their services to the acceptance of a cookie**. This would not only disproportionately interfere with the freedom to conduct a business and the freedom of contract, but also undercut the EU's competitiveness in the data-driven and knowledge-based digital economy.

DIGITALEUROPE is very concerned about suggestions put forward by the Article 29 Working Party that would prohibit consent in certain situations. We would like to recall that the consent requirements in the GDPR have been subject to very extensive debate and were as a result considerably strengthened. Indeed, the GDPR contains specific rules for the processing of special categories of data and new provisions were added to the law to address, among others, situations "when the processing has multiple purposes" or when a "performance of a contract, including the provision of a service, is conditional on consent". The strict interpretation of these rules is already considered by many practitioners as almost impossible to fulfil. Given that regulators take it as a given that the consent requirements in the privacy field should be interpreted in light of the GDPR, it seems **highly questionable why these rules would need to be re-written** , to address the same concerns, **although the GDPR provisions have not even been tested in real life**. Therefore, DIGITALEUROPE strongly opposes suggestions that describe circumstances in which consent would be prohibited.

It is important to recall that there are many applications and services that are offered free or low-cost to users due to the revenue gained through online advertising. Without this revenue, it would simply not be possible to offer free or low cost applications. **It cannot be the objective of the European Commission to make each and every website on the web a paid-for service.**

It should be clear that, provided users are given clear, upfront information about access and storage of their personal data on their device (including for advertising purposes), as required by the GDPR, it is valid to obtain their consent by their accepting such access/storage as a condition of the installation of the free or low cost application or access to the website. Uninstallation of the application (or ceasing to access the website) should be equally accepted as the mechanism by which users withdraw their consent.

Our members do take note of concerns related to tracking. However, it is important to underline that these concerns were at the heart of the debate leading to the adoption of the GDPR. Indeed, the **GDPR contains several**

provisions related to online advertising and profiling. It is important that these provisions are tried and tested in practice, before further rules and requirements are introduced.

DIGITALEUROPE fears that free or low cost services will cease to exist if the EU follows an overly rigid interpretation of the consent requirements of the GDPR, let alone add further restrictions in a new law. This will have a very substantive detrimental effect on the app industry as well as consumer choice.

8. Enforcement

Enforcement powers should be conferred on the public agency that is the most competent in the matter at hand. For the sake of consistency, and as far as information society services are concerned, matters related to personal data, including security measures related to the protection of personal data, should **solely be dealt with by national data protection authorities**, as per the GDPR.

9. Coherence & Harmonisation

The legal instrument outlining data protection and privacy requirements must ensure maximum harmonisation and consistent application and therefore a Regulation is preferable.

Ensuring coherence, consistency and harmonisation of legal requirements is particularly important for legislation that aims to or already covers online communication services, which are cross border and unlike traditional communication services are not regulated by national entities. In particular in these cases, any national fragmentation in the implementation and interpretation will lead to significant legal uncertainty for these service.

Should ePrivacy continue to complement and particularise data protection laws, then a **Regulation** would ensure better alignment and consistency with the recently adopted GDPR.

10. Conclusion

We believe that any review of the legal framework must be relevant, ensure consistency and avoid overlaps with other legal acts. All provisions must be carefully considered as to whether they are relevant or bring any value to the protection of citizens. Importantly it must ensure that it does not inadvertently lower or weaken the standard of protection it seeks to maintain and must acknowledge that the underlying technology or infrastructure that delivers a service matters as it affects the ability of a service to meet the legal requirements. We wish to stress that it is far more challenging (if at all possible) for an end-to-end encrypted OTT communication services to be designed to meet interception requirements.

As demonstrated above, we believe that the revision of the ePD needs to be undertaken with strong consideration to the GDPR and with the **aim to truly simplify the regulatory environment**. To the extent any of its provisions are still deemed necessary, all regulatory avenues should be explored. This includes **not maintaining a standalone piece of legislation.**

--

For more information, please contact:
Damir Filipovic, DIGITALEUROPE's Director (Digital Enterprise & Consumer Policy)
+32 2 609 53 25 or damir.filipovic@digitaleurope.org

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 62 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: FFTI
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: ICT IRELAND
Italy: ANITEC
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: TechUK