Position paper on the Proposal for an E-Privacy Regulation

The Developers Alliance represents software developers and the companies invested in their success. Alliance's members include businesses of all size, that are leaders in consumer, enterprise, industrial, and emerging software development, along with a global network of more than 70.000 developers.

Software developers are committed to the highest protection of their users' data and privacy, and the Alliance welcomes any efforts to streamline existing privacy rules and make them fit the digital age.

However, we believe that the ePrivacy Regulation will not deliver on either those objectives.
Hence, we encourage policy makers to re-evaluate the content of the proposal in order to:

Avoid further unnecessary constraints to the collection and processing of communication data and metadata

Articles 5, 6 and 7 risk jeopardising the ability of software to perform correctly and limiting the benefits deriving from collecting and processing data safely. This could put the future development of IoT and AI technologies at stake.

Re-think the proposed rules about the use of processing and storage capabilities of terminal equipment

Proposed articles 8 and 10 would impose severe restrictions on service providers' ability to process data. In addition, these rules would limit the use of technologies (like cookies or analytics services) that are key for small and micro businesses, that rely on "free" business models (ads-based or freemium).

Aim at creating full harmonisation of legal instruments regulating data management and data protection

A new discussion on issues such as profiling and advertising through article 10, already debated and regulated by the GDPR framework, would create confusion for small, dynamic businesses, especially those relying on ads-based business models.

{ I – PRIVACY IN THE DIGITAL AGE – INTRODUCTION }

The Developers Alliance represents software developers and the companies invested in their success. Alliance members include businesses, of all size, leaders in consumer, enterprise, industrial and emerging software development, along with a global network of more than 70.000 developers. The Alliance welcomes any efforts to streamline existing privacy rules and make them fit the digital age. However, we believe that the ePrivacy Regulation will not deliver on either those objectives.

During previous phases of the discussion, the Developers Alliance advocated for repealing the existing ePrivacy Directive[1], believing that sufficient protection is guaranteed by the GDPR and the NIS Directive, combined with a revised Electronic Communications Code. In fact, the GDPR already addresses issues such as consent, tracking, profiling, transparency and security standards.

On the contrary, whilst we fear that this proposal risks putting those principles in jeopardy, we are also dubious that the proposed regulation will help achieve better consumer satisfaction or protection. The Alliance observed that the impact assessment did not show a market failure big enough to justify stricter rules. More generally, the Alliance supports the Commission's Better Regulation agenda - which aims to reduce regulation, to the benefit especially of small industry players such as our members.

Therefore, the Alliance encourages policy makers to re-evaluate the content of the proposal.

We think the following issues deserve their attention:

- ✓ the **prohibition of collection and processing of communication data and metadata**: the provisions included in art. 6 would hamper the execution of basic communication services function and features, as well as put in jeopardy users' safety online;
- ✓ the **prohibition to "use processing and storage capabilities of terminal equipment**" and the prohibition to collect information from users' terminal included in art. 8, with the consequence that none of the apps could be technically provided to users' equipment;
- ✓ the **re-opening of the discussion on profiling and online advertising** through art. 10**,** which has been already debated and regulated by the GDPR; and
- ✓ **overly prescriptive obligations concerning privacy settings and engagement with users**, while the GDPR has already set out rules on both transparency and control.

Finally, we are extremely concerned about the very tight timeline imposed by the European Commission. Such a fast adoption of the regulation will not allow developers to have the time and informed understanding to allow compliance with the rules.

Thus, we would urge all decision makers not to rush into adoption. As detailed below, the proposal as it is would have severe consequences, which need to be properly assessed.

[1] Developers Alliance response to the Public Consultation "Questionnaire for the Public Consultation on the evaluation and review of the E-Privacy Directive"

{ **II – ISSUES and ANALYSIS** }

II (b) - Prohibition of processing of electronic communication data (article 6)

According to art.6, the processing of communication data is considered as an extraordinary action, only allowed in case the processing itself is strictly necessary for the performance of the service or for security purposes. Furthermore, art. 6 requests consent of all parties included in the communications in order to allow the processing.

Interestingly, this approach has been described as "protection against communication". In his piece E -Privacy Regulation: Nine flaws that should be corrected, Prof. Niko Harting explains that "interception and surveillance are serious interferences in confidential communications. Mere data processing does clearly not constitute such an interference. On the contrary: the "processing of electronic communications data is what telecommunication is all about".

In fact, the processing and aggregation of communication data enable software developers to create innovative products, including smart features, that are highly appreciated by the consumers. Consumers do not perceive communication products as tools that simply convey messages, but realize and appreciate the fact that electronic communication services engage proactively with them and offer services targeted to their needs.

The current proposed rules would restrict and discourage the development of features based on content analysis, from the more traditional (such as spam-filtering or fraud detection software) to the most innovative (applied artificial intelligence). Some of the many examples of industry leaders collaborating to accelerate the growth of artificial intelligence include:

- Google's TensorFlow, an open-source software library for machine learning;
- Yahoo's CaffeOnSpark, open-sourced for distributed deep learning on big data clusters;
- Facebook's use of Torch, an open-source development environment, for its machine learning and AI research.

Recommendation:

Follow the risk based approach outlined in the GDPR and allow the processing of electronic communication data based on the legal basis outlined in art. 6 of the GDPR to the benefit of software and app development. Any laws or regulations relating to Artificial Intelligence should mirror the 'light-touch' approach that has allowed innovation to flourish, must take into account the challenges of regulating a burgeoning technology, and should be sensitive to additional compliance burdens placed on small- and medium-sized enterprises.

II (c) - Regulation of terminal equipment (article 8, article 8. 1 (d))

Art. 8 prohibits the use of processing and storage capabilities of users' devices, as well as the collection of information from those. Such a prohibition gets slightly mediated by a list of six exceptions allowing partial data management (including end user's consent, according to art. 5 of the GDPR, the necessity of such processing for transmitting the communication or measuring web audience and the display of a prominent information notice ex art. 13 of GDPR) which, however, will not ensure full and correct performance of app/software.

To function, apps rely on the processing and storage capabilities of the device, otherwise, they would need to be downloaded again every time they are used. Moreover, apps need to collect certain information about the users' devices in order to ensure that the user gets the appropriate updates (which region it is in, what version of the

operating system is used, etc.).

In addition, whilst the provisions are very strict, the exception of "necessity" included in art. 8, 1 d) is not solid enough to justify a variety of cases where storage and collection of data from the equipment is key.

In fact, the meaning of "necessary" is not universally clear and the court interpretation tends to define it very restrictively. Consent may also not always be practical as most of the updates for security purposes happen automatically.

We reiterate the importance of maximum consistency of data/privacy protection rules and emphasise that the GDPR already provides the legal basis for using processing and storage capabilities or collect information from the device. We agree with the statement of the European Data Protection Supervisor affirming that "*the strict conditions under which a processing can take place are already set down in the GDPR*". We believe that reducing the range of legal basis for processing to the only consent is unreasonable.

In further details, the Alliance wishes to raise its concerns on the impact that these rules will have on crucial technologies for the software ecosystem, such as data analytics technologies and online advertising.

Article 8.1 d) reduces the scope for data analysis provided by third parties, allows processing and storage capabilities of terminal equipment only when:

- It is necessary for web audience measuring;
- the measuring is carried out by (only) the provider of the information society service;
- It is requested by the end-user.

Such a narrow scope would severely impact small digital businesses that rely on third party providers for services supporting business models, going far beyond the simple "web-site measurement". Those services are mainly B2B and are usually not requested by the user or carried out to the direct end-user's benefit. Some examples:

- user identification and retention
- investment return through the development of an efficient mobile marketing strategy
- product improvement and user experience design

In addition, art. 8.2 seems to add a further regulatory layer on the online advertising by imposing new obligations to request and offer information. We encourage policy makers to avoid adding new limiting provisions, provided the importance of an ads-based business model for the digital industry. We would like to underline the importance of the ads. 38% of worldwide developers base their business model on advertising, while only 21% are still profiting from downloads and 19% are looking for subscription revenue[2]. On top of this, the trend of adopting mixed business model is growing: in many cases, paid app business models are integrated with alternative ads-based models.

We also wish to flag that the GDPR already deals with profiling (in reference to advertising) and, depending on the consequences of such profiling, it imposes a strong right to object or consent. The GDPR also stresses the importance of transparency so that users "*know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising*".

[2] Vision Mobile blog,August 2016: Why are mobile developers so obsessed with advertising

Therefore, it is hard to understand why a paid-for model should be a preferable or even a viable option. The cost of setting up an infrastructure for payment would be high. There are also increased liability exposure and security risks that are inherent to collecting users' credit card information. Not least, the average user is not willing to pay for apps.

Recommendation:

The use of processing and storage capabilities of terminal equipment and the collection of information from users' terminal equipment should be allowed on the basis of the legal grounds outlined in Art. 6 of the GDPR.

II (d) – New cookies rules

The Alliance welcomes the Regulation's aim to revisit the existing rules on cookies, given the negative feedback received from both industry and consumers on their effectiveness. As a matter of fact, cookies have shown to impair user experience and to exasperate online interactions.

However, we would recommend to re-think the rules as included in the Commission proposal: designing an opt-in paradigm for consumer to be exercised at the very beginning of the online interaction would deprive the consumer of a granular control of data sharing while making obligations stricter and the scope wider.

Further to that, we believe that art. 10, as it reads today, creates uncertainty around the following key points:

- As the browsers provides the users with the privacy setting choices, relevant also for advertisement providers, the relation between the two players would need to be clarified further. Either through additional legislation or contractual agreements, this would translate into more obligations particularly burdensome for smaller businesses;
- Recitals 22, and in particular when it mentions the role of some apps as gatekeepers.

Recommendation:

Art. 10 and related recital should be amended profoundly in order to change today's opt-out paradigm and seek the right balance in transparency requirements. As currently drafted, the rules impose service providers to share and specify the risks of consenting to data processing, without encouraging them to explain also the benefits of such a decision. Therefore, the consumers are pushed towards the opt-out and are prevented from being fully informed about data processing and its positive consequences.

II (e) - Law enforcement access to data

The procedure established by art. 11 (2) of the current proposal might introduce unbearable notification procedures for software developers and publishers, especially for those with limited resources. The Developers Alliance worries that transparency requests, coming from all across the Union, would overwhelm smaller businesses. Therefore, we encourage policy makers to value the existence of one prevailing jurisdiction in order to ease the position of businesses and allow them to deal with any request efficiently.

Recommendation:

Repealing art. 11, or simplify jurisdictional criteria by introducing one-stop-shop.