The Commission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation Dedicated to ePrivacy in the European Union?

Giovanni Buttarelli*

In May 2018, we will welcome the application of the much-awaited General Data Protection Regulation (GDPR). This piece of legislation represents a landmark for fundamental rights in the Internet era. It is expected to strengthen the role of the individual data subject vis-a-vis the data controller and to bring transparency to the often opaque world of personal data processing. However, no matter how proud we may feel about this achievement, we must not forget that the EU legal framework would be incomplete without the Commission proposal for a Regulation on ePrivacy, meant to replace the current ePrivacy Directive as soon as May 2018. Indeed, the GDPR and the ePrivacy Regulation, although complementary to each other, will address different fundamental rights, they will have different material scope and they will apply to different actors.

As the proposed ePrivacy Regulation currently stands, it provides an ambitious attempt to safeguard privacy in the field of electronic communications. The choice of instrument (that of a regulation rather than a directive), the extension of scope to ‘over the top’ service providers (OTTs) and the proposed enforcement powers granted to supervisory authorities illustrate this ambition. Nevertheless, in order to complete the data protection and privacy framework of the European Union, the EU legislator must ensure that the final text actually delivers on this stated ambition.

Why Do We Need a Regulation Dedicated to ePrivacy in the European Union?

The proposed ePrivacy Regulation concerns processing of electronic communications data and information related to terminal equipment. Examples of the latter category include location and traffic data emitted by equipment such as smartphones and IoT applications. It is noteworthy to recall that the collection of location and traffic data formed the subject matter of the much controversial 2006 Data Retention Directive, which was declared invalid by the Court of Justice in its Digital Rights judgment in 2014. Retention of traffic and location data was again addressed late last year in the joined cases of Tele2 Sverige and Watson where the Court addressed national implementations of the Data Retention Directive. In both cases, the Court noted that these data make it possible to ‘draw very precise conclusions’ about the private lives of in-

* Giovanni Buttarelli, European Data Protection Supervisor.
DOE: 10.21352/edpl/2017/2/5
individuals subject to collection of data. Consequently, and as is expressly mentioned in recital 20 of the proposed Regulation, such data deserve enhanced privacy protection.

For many, the subject matter of the ePrivacy Regulation immediately raises economic and social questions and therefore triggers intense discussions on what one can and cannot do with collected data. Amidst these discussions, many tend to forget about the ultimate objective of ePrivacy rules: to secure natural persons’ right to confidentiality of communications. This right forms part of the fundamental right to protection of private and family life, enshrined in Article 7 of the Charter of Fundamental Rights of the European Union (the Charter), Article 8 of the European Convention on Human Rights and many national constitutions. The right to confidentiality of communications can hardly be overstated. It promotes trust in society and is essential for the functioning of modern societies where electronic communication has become an integral part of our daily lives. This fundamental right should always be our starting point when we engage in discussions on the proposed Regulation.

It is equally important to emphasise that the right to confidentiality of communications goes beyond compliance with rules for processing of personal data. The right to protection of personal data, set out in Article 8 of the Charter and particularised in secondary law such as the GDPR, is a distinct fundamental right. This right concerns the processing of personal data by a controller or processor. The proposed ePrivacy Regulation would require none of these elements but would apply to a broader range of data (electronic communications data, whether personal data or not) and to different actors (for example electronic communications service providers and software providers). It would also grant protection to legal persons in certain circumstances (just as the current ePrivacy Directive does). Compared to the GDPR, the ePrivacy Regulation would thus provide for more specific safeguards in situations where processing risks having an important impact on individuals. In other words, and as set out in the proposed Article 1(3), the ePrivacy Regulation aims not only to ‘particularise’, but also to ‘complement’ the provisions of the GDPR. Although the current ePrivacy Directive 2002/58 already provides individuals with a degree of protection in the context of electronic communications, its scope and provisions no longer ensure a sufficient degree of protection. Rapid technological developments and our virtually non-stop use of apps, services and connected devices have rendered provisions of the Directive - which did aspire to be technologically neutral - largely outdated. Moreover, once the GDPR becomes directly applicable throughout the European Union, the ePrivacy Directive and its many national transpositions may well turn out to be inconsistent with the general data protection framework. In light of all the foregoing observations, it is safe to say that without the proposed ePrivacy Regulation, the EU privacy and data protection framework would be incomplete.

**What Kind of an ePrivacy Regulation Do We Need in the European Union?**

In order to ensure an effective and workable reform of the ePrivacy framework, we need straightforward, sustainable and simple rules on ePrivacy. The proposed ePriva-
cy Regulation is an example of how the legislator seeks to keep pace with technological change. In the field of ePrivacy, we have seen this before. In 1998, the EU adopted a Directive on the processing of personal data in the telecom sector. The telecom rules were rewritten in 2002 in order to reflect the emergence of digital mobile networks. Seven years later, this ePrivacy Directive was amended by the so-called ‘cookies Directive’ in 2009. Now, in 2017, the legislator aims to regulate the development of new OTTs and tackle ubiquitous tracking of behaviour. At the same time, it is imperative that the proposed Regulation ensures consistency with the GDPR. As was the case with its predecessors, whenever personal data falls within the scope of ePrivacy, the ePrivacy Regulation will be *lex specialis* to the more general data protection rules. Hence, it is essential that the ePrivacy Regulation does not lower the level of protection of personal data ensured by the GDPR.

In order to ensure the right to confidentiality of communications, in Opinion 6/2017¹, the European Data Protection Supervisor (EDPS) has proposed that the ePrivacy Regulation should provide for standalone definitions that are suitable to a fundamental rights context yet consistent with the proposed European Electronic Communications Code (EECC). Currently, the proposed definitions rely too heavily on those put forward in the EECC and, as a result, risk lowering the level of protection vis-a-vis the ePrivacy Directive. The EDPS has also recommended a revision of the current phrasing of ‘end-user consent’ as it may suggest that others than the individuals who in fact use a service can consent to the processing of personal data on their behalf. Such an outcome does not reflect the kind of ePrivacy instrument we need in the European Union.

As I have suggested several times this far, we must ensure the necessary consistency between the ePrivacy Regulation and the GDPR. Although the proposal represents a step in the right direction, there is still room for improvement on this matter. The ePrivacy Regulation should provide for clear rules on the relationship between these two instruments. To ensure legal certainty, it should not be possible to process personal data collected in accordance with the ePrivacy Regulation on other grounds than those provided for in this particular instrument. In addition, consent provisions in the ePrivacy Regulation must meet the requirements of consent as set out in the GDPR. This means that in order to ensure that consent to processing personal data is freely given - and therefore consistent with the GDPR - the provision of a service should not depend on tracking. Individuals should not have to face privacy-invasive ‘take it or leave it’ situations. Instead, tracking walls ought to be prohibited. Similarly, device tracking should only be allowed with the consent of the user. Hardware and software providers ought to be obliged to provide privacy-friendly settings by default - providing users with a mere option to decide whether to allow third party access to their devices (as the Proposal currently reads) does not live up to the demands of privacy by default. Fi-

---

nally, provisions on restrictions must be brought into line with the GDPR. They must provide for suitable safeguards and thereby reach an appropriate balance between the rights of individuals and the interests of society.

Last but not least, the European Union needs a Regulation that enables businesses to develop creative personal data based services that are built on mutual trust. In this regard, businesses should become more transparent when it comes to data use and reuse. At the same time, individuals should be granted more control over personal data relating to them. More awareness of how service providers and other actors use data relating to individuals may be a first step in creating trust between users and market actors. Electronic communications service providers and other actors covered by the ePrivacy Regulation are in an apt position to develop relationships of trust with their customers. In such relationships, individuals may indeed be willing to share personal data for new innovative uses that benefit them as well as organisations adopting sustainable business models.

**Conclusion: Finding the Right Kind of ePrivacy Regulation for the European Union**

It is still early in the negotiation process, but certain themes are already emerging. These include the relationship with the proposal for the EECC Directive, the impact on Internet business models based on advertising, data retention as well as the role of data protection authorities. On the subject of data retention - which constitutes a restriction on the right to confidentiality of communications - it is important to emphasise that although the scope of the proposed ePrivacy Regulation would be wider than that of the current ePrivacy Directive, Member States are not thereby automatically free to extend existing or future data retention schemes. They would still need to demonstrate the necessity and proportionality of such measures, in line with the Charter and the case law of the Court of Justice. Also a comment on the role of data protection authorities in the field of ePrivacy is in order. By entrusting these authorities with the task of monitoring the application of the ePrivacy Regulation, the Proposal serves the interest of legal certainty and eases the practical implementation of the overall data protection and privacy framework in the European Union. It definitely reflects the kind of ePrivacy Regulation the European Union needs.

There is no doubt that the European Union needs a new legal framework for ePrivacy. We need straightforward, sustainable and simple rules that provide more clarity and better enforcement than the current regime. The proposed ePrivacy Regulation provides an ambitious attempt to do just that. Not only does it aim to tackle the challenges facing the current ePrivacy Directive but it also seeks to particularise and complement existing provisions in the GDPR. It is certainly a step in the right direction. However, ambitious objectives are not enough. The EU legislator must ensure that the final text actually delivers on them. Given the large number of stakeholders involved in this reform process, the legislator certainly faces a variety of arguments and suggestions on how privacy in electronic communications should best be protected. Regardless of how convincing these suggestions may be, it is imperative that the legislator never los-
es sight of the ultimate purpose of the Regulation: to embody a fundamental right en-
shrined in the Charter and numerous national constitutions - the fundamental right to
privacy and confidentiality of communications.