The new e-Privacy instrument – Finding the right balance between data protection and innovation

The telecoms industry is committed to contribute to a strong Digital Single Market, by building trust in digital services. For Telenor, the review of e-Privacy is a unique opportunity for a move towards a consistent privacy framework, for the **benefit of the consumers and businesses.**

The General Data protection Regulation (GDPR) is the landmark piece of legislation, which creates a future-oriented, technologically neutral framework, for the protection of personal data and privacy. It provides high level protection standards, whilst enabling innovation, essential to spur European competitiveness in data-driven markets at the global level, in Big Data, Cloud services, IoT and Platforms.

We urge the European institutions to look forward and to do a throughout assessment of the need and added value of any additional ePrivacy instrument in light of the GDPR. Maintaining a double set of rules without additional value cannot be considered an example of better regulation.

The review of the e-Privacy Directive should therefore ensure **alignment with the GDPR** on the processing of electronic communications data, and only deviate where it is necessary and proportionate. Telenor urges policy makers to strike the right balance to enable European businesses to innovate, whilst providing European citizens with a wide range of choice of trustworthy and the highest quality services.

The proposal for a new ePrivacy regulation from the Commission is a step forward on several fronts. The proposal has the potential to unleashing competition in the digital space through a more level playing field and to enable more innovation through more flexible rules. The legal form of a regulation is also a step forward as it will result in greater harmonization and fewer barriers to trade.

There are still improvements to be made in the proposal, and we very much welcome this chance to share our views.

The need to modernize the scope of application of the principle of confidentiality of communications

The proposed rules on the principle of confidentiality apply to electronic communications networks and services. By leveraging the proposed **definitions from the proposal for a European Electronic Communication Code**, the proposal **will create a more level playing field** and promote a consistent level of privacy protection in the digital sphere. Minor clarifications are necessary avoid problems of interpretation[1].

The proposed regulation also applies to 'services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service', thereby ensuring a small and appropriate scope adjustment compared with EECC to reflect the difference in object and purpose of the two sets of rules. There is still scope for improvement as a level playing field with the present proposal is still not created for competition with digital (content) services which are not ECSs, even though the associated content and metadata are equally high as the content and metadata of ECSs.

The Commission is taking an important step forward by suggesting that the enforcement of ePrivacy is done by the **same authority as the one enforcing GDPR**. This will increase predictability for investors,

[1] In art. 4(3)(c), the definition of electronic communications metadata should avoid referring to electronic communications network to ensure that metadata from other than the network layer are covered.

further European integration, promote optimal allocation of enforcement resources across sectors, and promote a level playing field.

It **is important to uphold the principle of confidentiality** of communications. However, it would be beneficial to include a clarification that insofar as providers of electronic communications services **act as end-users rather than providers** of electronic communications services, the strict rules of the ePrivacy regulation should not apply – how a customer service function can use electronic communications content as it is being received during a standard phone-conversation with a customer should for instance not be subject to the principle of confidentiality of communications and its limited exceptions.

Finally, we encourage that the wording of recital 14 is amended to exclude 'information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content' from the category of electronic communications metadata. To the best of our knowledge, there is no evidence to suggest that there is a need for sector-specific rules for such data, and the negative effects of applying rules that do not ensure the flexible approach of GDPR are significant.

Key benefits of GDPR in danger of being lost

The GDPR contains strong flexibility to balance the rights and interests of data subjects, controllers and third parties. As accounted for by WP29[2], the legal basis of '**legitimate interest**' plays an important role in data protection law by ensuring a legal basis of last resort for balancing of rights and legitimate interests, where other legal basis are not available. The legal basis of 'legitimate interest' strongly encourages a full realization of the principles relating to the processing of personal data (art. 5 GDPR) and other initiatives that can minimize risks to and empower data subject, as initiatives that work to that effect may cause the legal basis of 'legitimate interest' to become viable. At the same time, the legal basis of 'legitimate interest' provides for flexibility to meet unexpected situations, where the data controller and third parties have a legitimate interest to process personal data. Three examples of this could be initiatives by telcos to counter child abuse; Telenor, Harvard, Oxford and U.S. Centre for Disease Control's joint research in the spread of disease[3]; and situations where the called party has a legitimate interest in gaining access to information about the calling party. The 'legitimate interest' legal basis should exist both under the proposed articles 6 and 8.

GDPR provides the opportunity to use data for other than the purpose of collection (art. 6(4)), if the purpose is compatible with the original purpose. The data subject's reasonable expectations are an important factor in the assessment of if a purpose is **compatible with the original purpose**, and an important function of art. 6(4) GDPR is therefore to minimize how often data subjects have to take the necessary time to make an informed decision – it is the data subject's chance to say to the data controller, "please do not fill my life with burdens, think for yourself". An article equivalent to art. 6(4) GDPR does not exist in the proposed regulation. We expect that end-users will experience an overflow of consent requests, resulting in annoyance, provoking the creation of satisficing but overly simplistic decision-habits. It will therefore result in low quality decision-making and disempowered end-users if an article 6(4) GDPR is not included. In particular use-cases powered by (difficult to understand) new technology, with high potential to create value for end-users and society, such as big data analytics, are in danger of being undermined by low quality decision making. Inserting a paragraph equivalent to art. 6(4) into the proposed regulation would not only optimize the use of end-users' time, it would create better conditions for the realization of the potential of big data, increase the quality of decision making on remaining consent requests, and encourage use of privacy enhancing technologies and measures.

[2] WP29, Opinion 6, 2014. On the Notion of legitimate Interests oft he Data Controller under Article 7 of Directive 95/46/EC.

[3] See for instance our study done in Pakistan: http://www.gsma.com/mobilefordevelopment/programme/digital-identity/big-demand-for-big-data-new-telenor-study-on-dengue-fever-in-pakistan

Continuing with a related concern, the proposed art. 9(3) risks becoming an annoyance to end-users. We believe that the proposed provision risks creating **mail-boxes overflowed by reminders to renew consent**. We do recognize the need for end-users to not lose control by, for instance, forgetting what consents the end-user has given. However, we do not believe that the identified solution is going to create a good customer experience. Indeed, should the proposal become law, market based solutions to the problem would be foreclosed and we would never find a good solution.

A remaining need for modernization

While the proposal for an ePrivacy regulation provides important modernizations of the ePrivacy directive, such as deleting the itemized billing requirement, some elements remain in the proposal, which should be deleted. The rules on presentation and restriction of calling and connected line identification and the rules on incoming call blocking are overly prescriptive, they foreclose innovation and they limit testing of new business models. The proposal for instance requires that "[p]roviders of publically available number-based interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted calls by end-users" (art. 14). This **requirement removes the incentive for providers of electronic communications services to innovate** in new and better ways to limit the reception of unwanted calls. Research by Telenor is ongoing into how machine learning can be leveraged for the purpose of closing a well-known SS7 vulnerability by identifying suspicious (unreal) behaviour[4]. Such research has great potential and might be leveraged to deal with unwanted calls, but no individual provider of electronic communications services has a strong incentive to do research and innovate, if the field is regulated with a requirement to always provide "state of the art measures", maybe even free of change, even to business customers. There is a need for flexibility so that companies can invest in research that will cater to the needs of special segments which have an extra strong need for new features. The resulting innovation may over time become available to end-users who initially did not value the innovations sufficiently to be willing to pay for the research. Telenor encourages that stakeholders, if not seek to abolish the identified rules, then explore the consequences of abolishing the rules by limiting requirements to only apply towards natural persons.

[4] An example of behavior that may be identified as suspicious using machine learning could be that a phone one second is in Norway and the next in Bangladesh. Through machine learning, it would be possible to identify such behavior (and other less obvious attacks through SS7) and prevent the consequent leak of personal data.