BUSINESSEUROPE

16 May 2018

Non-paper: ePrivacy position summary

This summary sets out our main concerns in relation to the ongoing negotiations in Council on the ePrivacy dossier. Businesses acknowledge the need for an update in this area to enable a greater level playing field. It is also a chance to enhance user trust and confidentiality. But this must be achieved in a proportionate, robust and legally certain manner.

In the meantime, the General Data Protection Regulation (GDPR) will effectively achieve the objectives of this proposal until sufficient time is taken to fully understand additional solutions that are needed in this policy area. Rushing ahead with this proposal in the current manner that has taken place will hinder a vast number of sectors, particularly as this proposal will impact all businesses transmitting and storing any kind of data (personal data, machine data, meta data, content data and data of business and private communications).

We currently do not see the necessary improvements reflected in the latest discussion papers of the Bulgarian Presidency in Council. To make the proposal fit for purpose, please find some of our main points from our position paper (14 June 2017) below that still need acknowledgement:

***Align* with GDPR:** the ePrivacy proposal maintains a separate track of privacy law alongside the GDPR. It should compliment it through focussing on the principle of confidentiality of communications (art 7 Charter of Fundamental Rights of the EU) instead, it overlaps basic principles established in the GDPR itself, creating confusion and lack of legal certainty for data controllers as well as for data subjects. It should be consistent with GDPR.

***Remove* ancillary services:** the inclusion of communication services that are ancillary to another means is not suitable in this context. Virtually all players using some form of electronic communication within the delivery of their service are covered (even though not a primary function but rather an aspect for it to work). This will not achieve a level playing field.

***Remove* machine-to-machine (M2M) communication:** inclusion of the multitude of possible b2b entities that electronically interact throughout complex supply chains will greatly impact Europe's ability to digitalise. It would also be practically impossible and greatly burdensome to ensure automated consent is legally valid between two machines. Products and services containing an M2M platform should not fall within the scope of this proposal.

Case Examples: in **smart agriculture**, it would be unclear as to how sensors relaying information between one another in a self-provisioned manner with no obvious end-user could demonstrate that consent has been provided for this transmission to legally take place. For **connected cars** and **automated driving**, in a context with multiple data

controllers using the data for diverging purposes “legitimate interest” and “performance of a contract” seem to be the most adequate legal basis for the processing of personal data. However, both legal basis are only recognised in the GDPR (art 6(1)) but not in the proposed ePrivacy Regulation.

Widen ***permitted processing:*** digital services now offer various smart features and no longer just a single line of content communication. In order to continue delivering and improving these services for consumers, data processing needs to take place in an innovative manner. Diverting from the GDPR and overrelying on consent as the only legal ground for processing will severely restrict the ability for businesses to continue offering cutting edge services to consumers. The small list of exemptions will also not provide a flexible or robust instrument. Additional legal grounds for processing (eg. performance of a contract, compliance with a legal obligations, legitimate interest) and the principle of “compatible further processing” as set out in art 6(4) GDPR should be included.

Case examples: **employer** is responsible for its IT eco-system in terms of its security and privacy of individuals that use it (even in relation to this proposal!). This requires work-related software and products (eg. digital tools, apps, services, smart phones and tablets etc.) are updated with latest technologies. But this would be near impossible if companies are completely dependent of the consent of their employees (also questionable under the GDPR by the Article 29 WP Guidelines so other possibilities like “legitimate interest” should be possible even more so). Some **online providers** process communications in order to maintain public safety, as they need to detect terrorist content, child abuse images and spam or security threats. Consent is not an appropriate legal basis for such processes which involve bad actors.

Remove ***storage provisions:*** the use of many digital services rely on the ability for users to store their content. It is therefore impractical to dictate that once processed the data is anonymised or deleted. While we understand consumer interests in the storing of their data, the GDPR’s principles and rights do also apply for e-communications (eg. purpose limitation, data minimisation, storage limitation, right to erasure and objection). In fact, this proposal was originally only intended for data in transit.

Align ***Consent+ with GDPR consent*****:** the type of consent used in this proposal diverges from GDPR consent. Additional safeguards such as proof that anonymisation was tried and does not work, a data protection impact assessment was carried out and prior DPA consultation was taken. The number of digital services consumers are using is growing, only permitting this diverged version of consent as a basis for processing will frustrate that user experience and create confusion between this proposal and the GDPR.

Use ***quality over speed:*** with preparations for the GDPR ongoing and full application around the corner it seems unnecessary that this proposal is rushed, particularly when businesses cannot prepare to apply both sets of rules when they do not know where political negotiations on this file will land. Important aspects such as processing on the basis of consent could also be learnt from through the GDPR before being favoured in this proposal. The right to withdraw consent at any time is already possible under Article 7(3) of the GDPR and should also apply in the context of this proposal. Therefore, the introduction of an additional obligation to inform end-users at periodic intervals of 6 or 12 months of their right to withdraw consent is not justified. Co-legislators already deemed this unnecessary during the discussions over the GDPR as it was agreed such additional

obligations would impose additional administrative burdens while not granting added value to the end-user. The same reasoning should prevail here.

***Focus* on privacy settings through GDPR:** extremely prescriptive measures to stipulate how businesses offer privacy solutions to consumers will not enable a competitive environment and therefore improve privacy in a robust manner as technology develops. As users will be required to choose their settings as soon as they install their service they will not be able to understand implications of their choices or test what fits their situation. Overall, this threatens net neutrality as limiting the ability for websites to revenue their existence through advertising will create an internet of paywalls and exist only for users willing to pay for it.

Case Example: users do not pay attention to the details of their privacy settings but rather trust their purchase to do its job. Research carried out by KPMG has shown that less than 21% of people read privacy policies when installing software. Users are more concerned about privacy providing data rather than generic software installations or updates. It would also be confusing for users to distinguish between protection of tracked browser data and electronic services data (eg. websites) in order to consent based on an informed choice.

***Focus* on law enforcement access for GDPR:** with the overall goal of creating greater privacy and confidentiality for users it seems contradictory that this proposal will broaden the abilities of Member States to access user data beyond that of national security (eg. taxation, public health and social security). Businesses do not want to implement backdoor solutions to weaken the security of their technologies.

***Maintain status quo* on unsolicited communications:** only permitting businesses to market similar products online rather than any product the consumer could be interested in once the b2c relationship exists will disproportionately impact online market places. Many businesses rely on these modern advertising practices in order to gain new customers. This is particularly relevant to SMEs.

***Maintain status quo* publicly available directories:** only allowing directory services to exist on the basis of processing data by consent (opt-in) will damage existing business models. Many Member States permit opt-out measures for name/number searches. Adding additional steps to gain consent for each category of data and whether it is searchable even though end-users will already have the possibility to amend their data or delete it under the GDPR is overburdensome. Particularly due to the rise in popularity of search engines to carry out this task.

Focus on risk notification through the GDPR: businesses are implementing breach notification procedures as part of the upcoming application of the GDPR. Yet this proposal overlaps these provisions as they stipulate that businesses should inform users of risks that may compromise security in advance rather than focus on actual risks that have happened. Also, it seems counterproductive to release information on potential weaknesses and potential attacks when the networks might be more vulnerable, rather than after the event.

***