Notes of event - IIC UK, GDPR or Privacy, that is the question

5 March 2019

The meeting was introduced by highlighting that GDPR has been in play since 2016, while the existing ePrivacy Directive ('ePD') dates back from 2002. Even though the proposed ePrivacy Regulation– ('proposal' or 'ePR') meant to bring the existing ePrivacy regime in line with GDPR - was adopted by the European Parliament in 2017, a deal has yet to be found in Council on a 'general approach' that would then allow negotiations to start towards a final text.

This stalemate poses a particular problem for 'over the top' communications providers, as they were nicknamed by a participant, who are now in scope of the Electronic Communications Code, which guides the ePrivacy's scope of application. These 'OTTs' like Gmail or Hotmail are now classified as Electronic Communication Services in the ECC and thus, they are also under the scope of application of the ePrivacy Directive and must abide by its rules. Yet, the ePD was not written with OTTs in mind. Thus, there is no clarity on how OTTs can apply the ePD requirements designed for traditional electronic communications services. Although the European Data Protection Board (EDPB) is looking at releasing guidelines (opinion) about the interplay between the ePrivacy Directive and the GDPR, including whether 'GDPR' sanctions may apply for infringement of the ePrivacy , there is still much uncertainty on exactly which set of legal requirements must be followed by communications providers (online and traditional), including because the ePrivacy Directive is not always enforced by EDPB members but also communications regulators such as Ofcom..

Panellists then made introductory statements where they mentioned in particular that:

- The impact assessment by the European Commission for the eprivacy proposal was poor and did not cover many of the implications, some felt.

- In the past, joint work by several committees (IMCO and ITRE) on the e-privacy directivehad helped make ePD provisions balanced, simple and effective (although it was not clear what had been achieved with some of the provisions such as the cookie clause). GDPR won't be as easy to implement, which is problematic especially considering the size of the sanctions. Generally, the practicality of the proposal was in doubt, including:
  - The need to examine other legal bases other thanobtaining consent
  - How to treat communications as a platform, such as in the case of the content of an email feeding into an automatic calendar update
  - Where GDPR starts and ePR ends, during the multi-intermediary journey of data transmission (especially as the EP text doesn't make the distinction between 'data at rest' and 'data in transit', and the EU Council remains unclear on the issue).

- Concerns were expressed over 'Christmas tree' phenomenon for ePR, as had happened with GDPR, with the inclusion of all sorts of clauses not initially in scope of the legislation – for example, deletion of child abuse images, which a panellist wondered whether ePR was the right place to do it, and for which no impact assessment was done.

- Some felt that ePR should have been integrated in GDPR; however, ePR cannot be simply done away with, because it protects a different right to GDPR's focus on protecting personal data: the confidentiality of communications, also enjoyed by legal entities, not only individuals, which is also included in several countries' constitutions and court systems of most EU states. Plus, GDPR does not deal with intrusion or misuse of communications.

- Updatingthe ePR to include online communications is a specially difficult exercise because the delivery of a traditional phone call, central to the wording of the current ePD, is very different to how online apps like Facetime or Skype or IoT communications work. While the ePD does need updating, it isn't clear how the new proposal would work in practice, such as what would be the impact on IoT sensor data used in collaborative projects, or simply communications apps and email.

- While GDPR had been positive for cybersecurity by raising board-level awareness and diffusion of idea of cyber hygiene ; but there is a need for clarity on the ability to process data at scale, while protecting personal data and ensuring the confidentiality of communications. Processing for cybersecurity should be exempted from the ePR, and there are worries about the (adequacy of) treatment of AI data processing in the current proposal.

During the Q&A, these concerns were often repeated and commented upon by the audience, and other aspects were highlighted including:

- The need for privacy legislation to explain well what ‘harms’ are, which was also not really addressed in the initial impact assessment.
- How to ensure implementation and respect of the law when data may travel through borders and 3rd countries during their journey from one recipient to another.
- Whether we have yet or need certification for IoT privacy and security, and how it could be enforced, and whether certification should distinguish customer or enterprise IoT.
- The difficulty to obtain (or ensure) ‘informed consent’ for certain apps and services which lie underneath the visible Internet architecture, such as some that may be collecting and sharing browsing history.
- Conflict of laws : for example how to identify and remove terrorist and other harmful content if you can’t process the underlying communications data. While the EC’s proposed Article 11 of ePR mentions exemptions for security purposes, the provisions do not clearly encompass less clear-cut content issues such as hate speech.
- Whether the EU’s approach to regulation may be undermining Europe’s ability to compete with China and the US in (data heavy) emerging technologies such as AI. Conversely, some felt that trust was key to competitiveness as can be seen with the low take-up of autonomous cars, because some felt, consumers are not yet convinced that this technology is sufficiently safe and secure. It was noted that those that are suffering are start-ups in the data sector, who are increasingly shunned by investors weary of taking risks in the face of expensive GDPR, which thus has a deterring effect on innovation and entrepreneurship.
- A number of comments about the need for Data Protection Authorities (DPAs) should consult stakeholders more, when drafting opinions and beyond. There was some criticism that the EDBP seemed too busy engaging in the US Congress and elsewhere internationally to promote the take-up of GDPR in other jurisdictions, rather than engaging with European businesses and stakeholders.
- There is widespread consent fatigue already, resulting in no ‘meaningful’ consent being given by citizens-consumers.

In conclusion, there are still many areas to clarify in both the application of the current ePrivacy rules to the new players that have been brought under its scope and also in the proposal for an ePrivacy Regulation, and many concerns regarding the ease and efficiency of its implementation and enforcement. At the time of the event (and of writing the note) it was not clear whether the proposed ePR would be adopted by this Parliament, by the next Parliament or, due to the deadlock in the EU Council, the Commission would prefer to withdraw the proposal and adopt a new one in the next European Parliament. The IIC would therefore likely return to this issue soon in its upcoming programme in the UK and EU.