ministry of
digital government
and gender equality

Session I – A strengthened framework on cookies and online tracking, particularly for children and youth

The primary regulatory framework for the use of cookies and other tracking technologies is the ePrivacy Directive. The Directive requires providers of digital services, such as websites or apps, to obtain explicit consent from end-users before using cookies and trackers beyond those that are technically necessary. The rules are implemented and enforced at national level with limited EU level harmonisation and coordination taking place.

In 2017, the European Commission published its proposal for a new ePrivacy Regulation to replace the Directive. Among other things, it intended to update the rules in light of technological and market developments that had taken place since the Directive was last revised in 2009. 7 years later, however, inter-institutional negotiations have not lead to an agreement on the proposal.

In the meantime, the legislative landscape has undergone fundamental changes. In 2018, the GDPR entered into application and with the Electronic Communications Code, the scope of what constitutes an 'electronic communication service' in the ePrivacy Directive was broadened. In addition, milestone legislation such as the NIS2 Directive, the Digital Services Act, the Digital Market Acts, the Data Act, the Cyber Resilience Act and the AI Act came into place.

Beyond legislative changes, transformative technological and market developments have taken place. New players have entered the market, introducing new businesses models and technologies, coupled with an even more extensive use of tracking technologies. At the same time, well-known issues persists and have only increased in magnitude. These include the so-called 'consent fatigue', the prevalence of information overload and asymmetry, users experiencing dark patterns and non-transparent cookie banners, poor protection of children and youth, and a general lack of legal clarity and clear guidance.

Also, the use of third-party services, where data is collected and shared with a third-party for various purposes such as marketing or user profiling, have become pivotal on websites and apps. Recently, the Danish Agency for Digitalisation conducted two reports on third-party services on websites and in gaming apps, respectively:

- *Report on websites:* Analysing more than 11,000 Danish websites, 9 out of 10 uses third-party services from Alphabet (Google and Youtube), while around a third uses services from Meta (Facebook and Instagram). Importantly, these results reflect the use of third-party services *even before* the user has considered whether to consent or has navigated around the website.

- *Report on gaming apps:* The most popular free gaming apps in Denmark were analysed. For these apps, children and youth are considered the primary target group. In the analysis, all tracking, data collection, cookies, etc. were rejected if possible. However, in all of the analysed apps, third-party services collected data for marketing purposes. Facebook from all the analysed apps, Google and AppLovin from almost all, and Tiktok from nearly half.

The latter report highlights the importance of having a dedicated focus on children and youth, as they increasingly engage in the online sphere. More needs to be done in safeguarding their data and protecting their privacy as essential elements of their online safety. The issues with minors' consent is well known, where well-functioning and privacy respecting age verification could play a key role in protecting children from excessive data collection. Furthermore, it could be explored to restrict the use of tracking technologies for services that are primarily targeted at children and youth, such as certain games.

In terms of the way forward, addressing the issues at hand would require new legislation that updates the existing regulatory framework on cookies and tracking technologies outlined in the ePrivacy Directive. Considering the long-lasting deadlock on the proposed ePrivacy Regulation, a first step would be for the new Commission to withdraw the proposal. A way forward could then be for the new Commission to prepare separate legislation to address the particular issue of cookies and tracking technologies.

With this in mind, we pose three questions for debate at the D9+:

1. Do you agree that issues persists in the area of cookies and tracking technologies? If so, which are the most pertinent and problematic issues in your view?
2. Which specific measures, instruments, rules etc. could help address the issues at hand?
3. Do you agree that a separate proposal addressing this issue is the most effective way forward? If not, what could be an alternative way forward?