TIE Position on ePrivacy Regulation

3 October 2017

Toy Industries of Europe[1] (TIE) represents reputable toy manufactures in the EU. Our members have a longstanding commitment to making sure their toys are safe for children to play with. Play is changing and digital platforms are increasingly a part of children's play patterns. This means our traditional focus is expanding to ensure that the connected play experiences we create for children are appropriate, safe and secure too.

We welcome the modernisation of the European privacy framework. Especially the move towards a more harmonised approach that recognises the borderless nature of the digital world.

As they review the ePrivacy Directive, we call on policy makers to:

- Agree principle-based, future-proof and pragmatic solutions that work in complement to the General Data Protection Regulation (GDPR);
- Make sure that any specific measures taken to protect children's right to privacy are proportionate to the risk to their private life; in particular, these measures should not be detrimental to children's other rights, like freedom of expression and access to information;
- Be aware of unintended consequences of policy decisions that may result in more intrusive information requests from parents, a downgraded online experience for children, or loss of free content. In particular that children and their parents may be pushed towards alternatives that are less safe, and have not been designed with children in mind;
- Recognise the positive benefits of limited data collection activities in allowing companies to offer engaging and innovative digital offerings for children. Prohibiting all data collection is likely to lead to a significant decrease in the development of appropriate content and services for kids.

The ability to collect certain types of data plays a big role in being able to ensure fun and privacy-safe digital play experiences for children. Importantly, it means that the identity of a child is protected, whilst allowing companies to enhance and improve their online services for users.

- Cookies and persistent identifiers, such as IP addresses, are used to help make children's online experience safe, intuitive, personalised by:
    - Guaranteeing a secure browsing experience;
    - Making sure that content appears in a child's chosen language, and that they don't have to reset these preferences every time they visit a site;
    - Ensuring content, such as videos, load at the right speed for the browser or device a child is using;
    - Facilitating navigation across a website;
    - Allowing a child to anonymously register with only a first name, or an anonymous user name, and a password, to "remember" the child when using a site and personalize their choices in a privacy-friendly way;

[1] TIE's membership includes international companies and national associations, together representing 80% of the EU toy sector.

- Remembering how far a child has progressed in a game, so they don't have to start from scratch if they take a break from browsing or come back in a few days to play again;
- Enabling the child to personalise the layout and look of a website – their preferred colour scheme for example;
- Providing suggestions from exciting new content – such as recommendations for videos or games based on the child's previous visits to a site;
- Collecting user statistics and aggregating information about how the site is used to make improvements to the services and content offered – making sure that search tools provide the most relevant results, for example.

This type of data also allows business to maintain, analyse and protect the security of their digital properties, protect their intellectual property, protect against spam, or address technical bugs and issues, as well as cap ad frequency (where sites are ad-supported).

In short, data is used for a range of legitimate business activities that are fundamental to the smooth functioning of the Internet, the quality of the digital service, and the individual user's experience. Allowing this type of use as long as the data isn't linked to other types of personal data strikes the appropriate balance between usability and privacy.

The General Data Protection Regulation (GDPR) already sets out strict standards for processing children's personal data, including:

- A wide-ranging definition of what counts as personal data – IP addresses and anonymous usernames are both considered as personal data under the GDPR;
- The requirement that companies carry out a risk assessment before they process children's data;
- Firm limitations on requiring a sound legal basis for processing children's personal data;
- Making parental consent necessary in most instances when children's sensitive personal data is processed;
- Prohibition on profiling of a child;
- Robust emphasis on the principles of privacy by default and design as well as minimisation of the collection of personal data.

Finally, sectoral standards set by the European Interactive Digital Advertising Alliance (EDAA) stipulate that children's data should not be collected for retargeting purposes or to serve them online behavioural advertising.

<u>Recommendation</u>

We therefore urge caution in the ongoing compromise discussions and the subsequent vote on the Report in the LIBE committee next week. Rules that are proposed with the best intention of protecting children may, in reality, lead to a decrease in fun and privacy-safe digital play experiences for children. Paradoxically, this could end up pushing children towards alternatives that are less safe, and have not been designed with them in mind.