54

BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 15:55
To: Verweij, Ellen
Subject: FW: Contribution to DAPIX discussion on Chapter II, Article 8
Attachments: Coppa - A Case Study for Parental Consent.pdf

Follow Up Flag: Follow up
Flag Status: Completed

From: [redacted] [mailto:[redacted]]
Sent: woensdag 14 januari 2015 13:13
To: Kaai, Geran
Subject: Contribution to DAPIX discussion on Chapter II, Article 8

Dear Geran.

Happy New Year. Ahead of DAPIX discussion this week, we wanted to urgently share our thoughts in relation to **Article 8, governing parental consent for personal data of children under 13**.

We are in full support of the Regulation's objective to provide specific protection for children and to involve parents in their children's online activities. The challenge we face is how to ensure that parents' consent is requested and respected when their children's interests or their fundamental rights and freedoms are genuinely at risk. It is important that we avoid excessive rules which could result in a dramatic reduction of child-appropriate services online and could seriou[redacted] impinge on children' ability to benefit from information society services as a whole. **In other words, a[redacted] based approach to the protection of children's data.**

1. Firstly we would like to draw your attention to a new proposal for a Paragraph 1a. to be included in Article 8. The Paragraph reads: **1a. Consent to the use of personal data of minors for the purposes of marketing or creating personality or user profiles shall be invalid.** [redacted]

We are concerned about the addition of this Paragraph for **three central reasons**:

a) Firstly this paragraph creates the concept of **"invalid consent".** In other words, even in a situation where legitimate consent is obtained, this could somehow be overridden and deemed "invalid". This is a dangerous precedent. The concept appears to contradict one of the fundamental principles of the GDPR, which is that consent is a key legal basis for processing and a critical form of positive expression by the data subject that processing of data can take place. To suggest that there exists a situation where appropriately obtained consent could be deemed "invalid" undermines the very principle of requesting for consent in the first place.

b) The use of the term **"minors"** is also unprecedented in this Regulation and the creation of a new target age group may lead to confusion. It is acknowledged throughout the document that "*Children deserve specific protection of their personal data*". In Article 8 Paragraph 1 specific protection has been given to "*children under the age of 13*" by requiring parental consent for the processing of their data. This at least brings a degree of consistency between the GDPR and COPPA in the US. There is no reference anywhere else in the GDPR to the concept of minors.

   a. The inclusion of this term would create a situation where a digitally savvy 17 year old will have to seek parental consent for the processing of their data, even if this data is neither sensitive nor having significant or legal affects. Cutting users as old as 17 from most digital services (accessing cultural goods, playing games, interacting via social networks) is greatly disproportionate and would severely

undermine users' freedom to enjoy the internet as we know it. **We do not believe this is practical, desireable nor appropriate as part of a risk-based approach.**

c) Singling out **"marketing"** creates an additional and discriminatory tier within Article 8, with no clear justification nor evidence for doing so. The GDPR aims to be both tehnology neutral and horizontal in its application and should apply this consistently. There is no evidence to suggest that data collected for purposes of marketing uniquely poses a greater risk to the data subject and, as such, there appears no justification for special restrictions on this sector.

As such we would strongly encourage the removal of this Paragraph 1a of Article 8.

2. In the context of COPPA, there was a clear recognition that, for this to achieve the desired balance, **the type of parental consent needed should be dependent on the type(s) of data collected, and whether and how the data will be shared**. For example, no parental consent for a child-directed website is required to collect **anonymous** or **pseudonymised** information. This allows children to participate in fun and engaging activities in a manner that does not pose a privacy risk. The rule also avoids that more information from parents is collected than they would otherwise need to allow children to even access the site. Without this flexibility, we risk ending up with an unpractical situation where children and parents do not cooperate and business has less and less incentive to offer child-oriented online content. The attached document provides more detail on the approach adopted within COPPA.

We have included recommended text at the bottom of the email which we believe would create a more **proportionate, workable article, whilst respecting the principle that children deserve specific protections**. As you will see we are broadly supportive of Councils proposal for amendments.

If you have any questions do let me know.

Best,

[redacted]
Public Affairs

World Federation of Advertisers
Avenue Louise 166 - 1050 Brussels
Phone: +32 (0)2[redacted]

Children and the General Data Protection Regulation

Article 8 - Wording suggestions

Proposal from the European Commission, as amended by the Council, the EP and our proposal

(29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. **Where data processing requires parental consent, methods of consent should be proportionate to the type of information collected and to the level and nature of the risks involved. Providers of information society services to children under 13 and other stakeholders should be encouraged to develop codes of practice for parental consent that meet the objectives of this Regulation and respond to evolving technological changes.**

***Article 8** – Processing of personal data of a child in relation to information society services*

1. **Where Article 6 (1)(a) applies** ~~for the purposes of this Regulation~~, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent, **proportionate to the data collected and to the level of risk involved,** is given or authorised by the child's parent or **legal guardian**. The controller shall make reasonable efforts to **verify in such cases that** ~~obtain verifiable~~ consent **is given or authorised by child's parent or guardian**, taking into consideration available technology, **without causing otherwise unnecessary processing of personal data**.

~~1a. Consent to the use of personal data of minors for the purposes of marketing or creating personality or user profiles shall be invalid.~~

2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

3. ***Member States and the Commission shall encourage information society services providers to develop common standards further specifying the criteria and requirements for the methods to obtain parental consent referred to in paragraph 1.***

Comments on the US experience with parental consent
From Toy Industries of Europe (TIE), and the World Federation of Advertisers (WFA)

The Proposal for a Data Protection Regulation lays down the broad principle that data collection for children under 13 would require parental consent, but fails to give detail on how and when this provision would apply. The US experience with parental consent under the Children's Online Privacy Protection Act (COPPA) provides for a useful precedent. It is often referred to as a valid and workable mechanism to increase children's privacy online.

Importantly, the text of COPPA contains a series of elements that are key to a workable and meaningful solution. Such elements are currently absent from the EU proposals. Without this flexibility, we risk ending up with an unpractical situation where children and parents do not cooperate and business has less and less incentive to offer child-oriented online content.

Even with the flexibility of the US system, our businesses have seen a very significant 'dropout' of children (and their parents) once consent is required, even for sites with robust data protection policies and no risk to the child's privacy was ever present.

What keeps the parental consent requirements (just) workable in the US?

1. There is a clear recognition that **the type of parental consent needed depends on the type(s) of data collected, and whether and how the data will be shared**. Allowing a child to play games at a website where its contact details will go no further should not require verification procedures equal to those necessary to open a bank account.

2. No parental consent for a child-directed website is required to collect **anonymous** or **pseudonymised** information. This allows children to participate in fun and engaging activities in a manner that does not pose a privacy risk. The rule also avoids that more information from parents is collected than they would otherwise need to allow children to even access the site.

3. No parental consent is required when companies collect certain data to support their **internal operations** such as maintaining or analyzing the functioning of the website or online service; authenticating users; personalising content; protecting the security or integrity of the user, website or online service etc.. This kind of data is usually associated with an IP address. If a company cannot provide appropriate support for their sites, evaluate the popularity of their digital offerings etc, they will often have no incentive to offer child-directed content so limitations here would lead to less content geared specifically to children.

4. **Filtering** (which preserves anonymity) is recognised as a legitimate and effective tool to prevent children from publicly disclosing personal information. To require parental consent for these routine businesses activities that support internal operations, sites will have to collect more information from children and parents, unnecessarily burdening privacy. This would be a disproportionate cost and burden, leading to less content geared specifically to children.

5. The collection of a child's online contact information for **one-time use** is allowed when the sole purpose of the collection is to respond to a child's request. The information may not be used to re contact the child or for any other purpose and may not be maintained in a retrievable form by the service provider. This allows children to interface with a website to ask for technical support or homework help, since the service provider otherwise would not have the authority to respond to the request if it has not obtained parental consent.

6. The collection of a child's and parent's online contact information for **multiple online requests where the information is not used for any other purpose or disclosed to 3rd parties** does not require parental consent, only parental notice. This avoids complicating the user experience and a potential overburdening of parents with unnecessary parental consent requests for activities that do not involve a privacy risk to children. Instead, the service provider simply notifies the parent and provides an opportunity for the parent to refuse permission. This enables the signing up to e newsletters or other periodic communications where experience shows that this does not result in privacy risks.