10

BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 15:54
To: Verweij, Ellen
Subject: FW: Contribution to DAPIX discussion on Chapter II, Article 8
Attachments: Coppa - A Case Study for Parental Consent.pdf

Importance: High

Follow Up Flag: Follow up
Flag Status: Completed

From: BRE-JUS
Sent: dinsdag 3 februari 2015 15:36
To: Grave, Martijn-de; Ruiter, Mieneke-de; Alink, Marnix; Kaai, Geran; Sorel, Alexander; Luijsterburg, Sander; Zwart, Jan; Kroner, Laetitia; Leenders, Sophie; Rip, Jet; Kellij-Smit, Nanda
Subject: FW: Contribution to DAPIX discussion on Chapter II, Article 8
Importance: High

Van: [redacted]
Verzonden: dinsdag 3 februari 2015 15:35:50 (UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Aan: BRE-JUS
Onderwerp: Contribution to DAPIX discussion on Chapter II, Article 8

Beste mevrouw Gevels,

Ik zou u zeer dankbaar zijn indien u dit kan doorsturen aan de heer Kaai, zoals telefonisch besproken, het is spijtig [redacted] genoeg wel hoog dringend.

Geachte mijnheer Kaai,

Ik schrijf u uit naam van de Toy Industries of Europe (TIE), één van onze leden is de ORNES, de Organisatie van Nederlandse Speelgoedleveranciers. Ik had een vraag over artikel 8 in de Data Protection Regulation (DPR) die naar het schijnt opnieuw besproken zal worden in de DAPIX-groep deze week. [redacted]

Als verantwoorde speelgoedfabrikanten steunen wij ten volle de opzet van de DPR om speciale bescherming voor kinderen te voorzien en ouders bij de online-activiteiten van hun kinderen te betrekken. De uitdaging zal zijn ervoor te zorgen dat de toestemming van de ouders gevraagd én gerespecteerd wordt wanneer het belang van de kinderen inderdaad op het spel staat. Echter, we moeten ook aanvaarden dat er verschillen zijn in risico en dat niet alle data even gevoelig zijn. We moeten vermijden dat overdreven regelgeving kinderen in feite zal uitsluiten van de online wereld in plaats van hen beschermen.

Wij vrezen dat zoals het artikel momenteel geschreven is, onschuldige data die een service/content provider (bv de ontwikkelaar van een educatief spel dat kinderen leert tellen) toelaat zijn programma te verbeteren, te personaliseren (het bijhouden van een score tijdens een spel of het laten doorgaan naar een volgend 'leerniveau' bijvoorbeeld) aan het kind ook verifieerbare toestemming van de ouders nodig zou hebben. We zouden pleiten voor een aanpak die het risico

i.v.m. data privacy weerspiegelt. Er zouden handelingen moeten zijn die bijvoorbeeld géén verifieerbare toestemming ('verifiable consent') nodig hebben, maar enkel bijvoorbeeld een korte communicatie naar de ouders toe, om hen te laten weten bijvoorbeeld dat hun kind op een bepaalde website een spelletje speelt. Het is ook bijzonder moeilijk om vanop een afstand écht 'verifieerbare' toestemming te geven, we moeten pragmatisch blijven.

In de VS bestaat COPPA (Children's Online Privacy Protection Act). De COPPA tekst zegt ook dat er een evenwicht moet bestaan tussen het beschermen van kinderen en ervoor zorgen dat ze niet uitgesloten geraken van online diensten die uiteindelijk specifiek voor hen ontworpen werden. COPPA stelt dan ook duidelijk dat het type van ouderlijke toestemming moet afhangen van het type data dat verzameld wordt en óf en hoe die data gedeeld zullen worden. Bijvoorbeeld, er is geen ouderlijke toestemming nodig indien het om 'anonymous' of 'pseudonymised' informatie gaat want dan is er immers geen privacy risico. Ik voeg hierbij een one-pager over de flexibiliteit die COPPA toelaat, om ervoor te zorgen dat de ouderlijke toestemmingsregel écht zou werken. We weten immers allemaal dat als hij té excessief is, hij omzeild zal worden door kinderen én ouders maar wél een kopzorg voor de bedrijven zal blijven.

Ik wil nogmaals aandringen dat we flexibiliteit nodig hebben om ervoor te zorgen dat kinderen én hun ouders willen samenwerken aan een beter data protection-beleid en ervoor te zorgen dat onze leden het interessant blijven vinden om online diensten aan te bieden die specifiek voor kinderen ontworpen werden.

Een tweede punt dat ik zou willen aanhalen is de recente toevoeging van het 'invalideren' van toestemming indien het om publiciteits- of 'user profiling'-doeleinden gaat. Dit lijkt ons ook gevaarlijk: user profiling is nodig om online inhoud relevant te maken voor de bezoeker (denken we terug aan de score tijdens een spel) en wat zou 'marketing' dan precies inhouden? Is het online spelen van een spelletje Monopoly publiciteit voor het echte gezelschapsspel? Kan dat dan niet meer?

Ik ben zo vrij hieronder een verbetering van de tekst te opperen die volgens ons een meer proportioneel en werkbaar artikel zou opleveren, geheel het principe respecterend dat kinderen speciale bescherming nodig hebben.

Het zou fantastisch zijn mocht u even de tijd hebben dit door te nemen en mocht ik uw medewerkster zeer binnenkort kunnen contacteren om te verifiëren wat de Nederlandse positie is i.v.m. dit alles.

Met vriendelijke groeten en bij voorbaat bedankt voor uw interesse,

[redacted]

[redacted]
Director General

Toy Industries of Europe (TIE)
Boulevard de Waterloo 36
1000 Brussels
+32 2 [redacted]
Do you know how safe toys are? Watch this short video to find out!

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

Recital 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 the 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.