Children’s data protection and parental consent

A best practice analysis to inform the EU data protection reform

October 2013
© Advertising Education forum
Table of Contents

Executive Summary ............................................................................................................................................. 3
Introduction .......................................................................................................................................................... 4
I. Parental Consent in the General Data Protection Regulation Proposal ................................................. 6
II. Current Industry Practices in the EU ............................................................................................................. 8
III. Global legislative landscape on data protection of children ................................................................. 10
    1. Europe .......................................................................................................................................................... 10
    2. Asia Pacific ................................................................................................................................................ 10
    3. North America ............................................................................................................................................ 11
        3.1. The 1998 Children’s Online Privacy Protection Act (COPPA) ...................................................... 12
        3.2. COPPA 2.0. ........................................................................................................................................ 14
IV. COPPA in Practice – some examples ........................................................................................................ 26
V. Lessons from COPPA .................................................................................................................................. 34
VI. Recommendations for the EU .................................................................................................................. 37
List of Sources .................................................................................................................................................... 38
Executive summary

In January 2012, the European Commission published a comprehensive reform of the data protection rules in the form of a Data Protection Regulation. According to the proposal, for the first time ever, the EU may be enforcing special data protection rules for children, including a provision that would require organisations to obtain parental consent for collecting and processing personal information for children under the age of 13.

This new provision could significantly affect the way children interact with new media, and could greatly impact businesses and the various organisations offering content for children online and offline. Although the large majority of the industry appears to be in favour of enhanced data protection for children under 13 and has already put in place voluntary safeguards, an ill-conceived regulatory provision could dramatically change the landscape of information society services available for children.

At this point, the proposal does not stipulate how verifiable parental consent should be obtained. It sets down a general principle, but invites the European Commission to adopt a “delegated act” – a form of executive decree – to determine, after the adoption of the Regulation, the technical elements to implement this article. Such a procedure is lengthy, opaque, and does not offer the immediate legal certainty that economic operators will need, once the Regulation is adopted, to continue communicating with children.

The purpose of this piece of research is to inform ongoing discussions on the best methods to obtain parental consent. Looking at the available evidence and learning from the experience of other regions of the world, this research tries to identify the best means to obtain parental consent in a meaningful, time efficient and practical way.

On the basis of a comprehensive analysis of industry best practice and existing legal frameworks in third countries (chiefly in the US), AEf makes the following recommendations:

1. Determine specific criteria to define what constitutes “information society services directed to children”. Children should be defined as under 13, according to international and EU best practice.

2. Propose a non-exhaustive list of parental consent methods, including the so-called sliding scale method. This method is considered as the most proportionate, cost effective and time-efficient method to obtain a parental consent.

3. Include built-in incentives for industry to develop new, more efficient methods of obtaining parental consent.

4. Clearly specify that parental consent requirement is restricted to websites directed to children or with “actual knowledge” of dealing with children under the age of 13.

5. Identify limited exemptions for scenarios with minimum or no privacy risks, where collection of children’s personal information would be made possible without parental consent.

---

1 European Commission (25 January 2012), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on free movement of such data (General Data Protection Regulation), 2012/0011 (COD), available online here, last accessed on 25 September 2013
Introduction

In today’s rapidly evolving digital era, children become technologically savvy at a much younger age and start using the Internet at increasingly early ages and much more often. Research conducted in the US by Common Sense Media think-tank reveals that 22% of children aged between 5 and 8 use a computer at least once per day, and 46% use a computer at least once a week.\(^2\) Children aged between eight and 10 spend around 46 minutes online per day. Their preferred activities include watching videos, playing games or chatting with their friends. Reportedly, 45% of 12 years old use a social networking site to communicate with their friends and family.\(^3\)

A survey conducted in the EU in October 2012 in 25 European countries by the London School of Economics revealed that 60% of children aged nine to 16 use the internet almost daily.\(^4\) Children reported using the internet mainly for school work (85%), playing games (83%), watching videos (76%), or for instant messaging (62%).\(^5\) On average, children aged nine to 16 spend 88 minutes online every day.\(^6\) Interestingly, children in the EU also start using the internet at an older age than American children - on average around the age of nine - \(^7\) while in the US children start consuming digital media as young as two or three years old.

As children are increasingly exposed to social networks and online activities, they are also exposed to greater risks on the Internet, especially through the inadvertent disclosure of their personal contact details. Children younger than 11 reported to be less aware of privacy settings, while only 26% of children aged between 11 and 16 said they take online privacy precautions.\(^8\) Young children may not, in most cases, understand the nature of the information being sought or the intended purposes for collection. They represent a vulnerable group, and should be protected accordingly. Therefore, soliciting personally identifiable information from children, such as full names, addresses, email or phone numbers, should trigger special privacy and security concerns, especially where this information could be publicly disclosed.

In January 2012, the European Commission published a comprehensive reform of the data protection framework in the form of a Data Protection Regulation (2012/0011), hereafter referred to as the DPR.\(^9\) It aims to replace the current Data Protection Directive of 1995 (Directive 95/46/EC), which does not include any specific requirements concerning children. The new proposal, the DPR, would require organisations to obtain parental consent for collecting and processing personal information of children under 13. This would bring the EU legislation in line with the United States’ Children’s Online Privacy Protection Act (COPPA), albeit with substantial differences.

\(^3\) Amanda Lenhart, et al. (2011), Teens, Kindness and Cruelty on Social Network Sites, Pew Research Center, p.17
\(^4\) Leslie Haddon and Sonia Livingstone (2012), EU Kids Online: national perspective, EU Kids Online, the London School of Economics and Political Science, London, UK, available online at [http://eprints.lse.ac.uk/46878/1/EU%20Kids%20Online%20national%20perspectives%2028lsero%29.pdf](http://eprints.lse.ac.uk/46878/1/EU%20Kids%20Online%20national%20perspectives%2028lsero%29.pdf), last accessed on 26 September 2013
\(^5\) Ibid. p.3
\(^6\) Sonia Livingstone, et al. (2011) EU Kids Online, the London School of Economics and Political Science, London, UK, available online at [http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%202009-11/EUKidsOnlineIIReports/Final%20Report.pdf](http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%202009-11/EUKidsOnlineIIReports/Final%20Report.pdf), last accessed on 26 September 2013
\(^7\) Ibid. p.5
\(^8\) Ibid. p.2
\(^9\) European Commission (2012), op.cit.
Beyond the general provision stipulating that personal data of children under 13 requires verifiable parental consent before collection, the proposal does not specify how parental consent should be sought and obtained, nor how it can be “verifiable”. The proposal contains a provision by which the European Commission would be entrusted to adopt a “delegated act” – a form of executive decree – to define the technicalities of the requirement. Delegated acts can be used to amend or supplement non-essential, but potentially important technical elements of a legislative act. They are adopted autonomously by the Commission, but both the European Parliament and the Council retain some very basic scrutiny powers.

The internet is an environment where children can develop their creativity, learn and have fun. Data from the EU already shows that children primarily engage in these types of activities.10 The industry also seeks to provide vibrant, fun, engaging and educational on-line content, especially for children and teenagers. Website operators and providers of child-oriented content are concerned that excessive data protection rules, designed without input from the industry, may bring unnecessary burdens without providing a safe environment for children.11 Data protection requirements should not discourage engagement with children online, but should seek to offer a safer environment.

This research aims to inform future discussions on the best means to obtain parental consent in a meaningful, time efficient and practical way. The objective is to provide evidence-based best-practice solutions that could form the basis for a future framework on this issue.

To achieve this, the current legislative landscape will first be analysed. The main focus will be on the United States which has, through the Children’s Online Privacy Protection Act (COPPA), implemented a comprehensive framework of practices governing rules on parental consent. The new rules proposed by the Federal Trade Commission (FTC), unveiled in December 2012, together with contributions submitted by industry leaders, think-tanks and consumer groups as part of the public consultation on the COPPA review, as well as academic evidence, will be closely reviewed.

We will then take a look at how market leaders have implemented current requirements with respect to data collection from children under 13 in order to determine best-practices guidelines for the European Union market.

---

10 Leslie Haddon and Sonia Livingstone (2012), op.cit., p.3
11 A common estimate is that the cost of complying with COPPA could be as high as $US5 per child. Source: https://www.fredlaw.com/articles/ebusiness/ebus_sp01_seh.html; last accessed on 8 July 2013
I. Parental consent in the General Data Protection Regulation proposal

The current EU data protection rules date back to 1995 and are based on the principle of ensuring the highest level of personal data protection. In practice, data can only be processed if an individual has given his/her consent or if the processing is necessary. The legislation is currently issued under the form of a Directive, giving member states some autonomy in the exact rules they adopt. This means that companies may face different rules and sanctions in different EU states.

The European Commission published its proposal to review the European Data Protection Directive in January 2012. The legislative package aims to harmonize legislation across the EU and to ensure that a single set of rules applies to all member states, thus effectively replacing the patchwork of existing national laws.

The objective of the General Data Protection Regulation (DPR) is to protect the individuals’ right to personal data and to ensure the free movement of personal data in the single market. The DPR applies to any collection or processing of personal data, whether on or offline, and it applies if the “data processor” (i.e. the organisation) or the “data subject” (i.e. the individual) is based in the EU. The DPR also envisages that valid consent must be made explicit and that consent can be withdrawn at any time.

At the time of publication of this research, the proposal is still being discussed, and the prospects of an adoption before the end of the current European Parliament’s mandate (April 2014) are becoming less realistic.

Importantly, with the revision of the Directive, the European Commission takes a step forward in protecting the privacy of children online. While the 1995 Data Protection Directive does not provide specific requirements for children, the new proposal would require website operators to obtain verifiable parental consent to collect and process the personal information of children under 13.

Specifically, article 8 of the proposal reads as follows:

1. 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 is given or authorised by the child’s parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in paragraph 1. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.

4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

---

13 Ibid., §1
14 Ibid., §7.3: “The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal”.

Children’s data protection and parental consent © Advertising Education forum
According to the proposal – provided it is adopted as such and not amended, the requirement to obtain parental consent for data of children under 13 will apply to all organisations offering information society services “directly to a child”\(^\text{15}\) – where a child is defined as anyone under 18, but does not define what constitutes services directed at children.

According to Article 4 of the DPR, “personal data” refers to any type of information such as “an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person”\(^\text{16}\), and “processing” personal data is defined as any action involving “collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction”\(^\text{17}\).

The requirement sets the age limit of 13 to obtain parental consent. However, Article 4 of the DPR defines a child as “any persons below the age of 18 years”\(^\text{18}\), meaning that the rule would also apply to websites targeting teenagers primarily, when they collect personal data from children under 13. Some Members of the European Parliament have also proposed to increase the age requirement for parental consent to 18.

At this point, the DPR does not specify how parental consent will be implemented and delegates the Commission to propose guidelines (paragraph 2), and possibly adequate methods taking into consideration the “available technology”. This raises a lot of questions: When should parental consent be sought? How can operators ensure that it is fully “verifiable”, as provided in the DPR? Should operators seek to get more personal data in order to adequately identify a child and therefore ask for his/her parents to give consent? Must consent be sought for every interaction, or once and for all?

\(^{15}\) Ibid., §8.1
\(^{16}\) Ibid., §4.1 and §4.2
\(^{17}\) Ibid., §4.3
\(^{18}\) Ibid., §4.18
II. Current industry practices in the EU

Although the 1995 Directive does not envisage special rules for children, it allows Member states to adopt stricter rules. Among all 28 Members of the EU, Spain is the only country to have taken advantage of that possibility, by adopting in 2007 a Royal Decree requiring parental consent for the collection of data of children under 14 years old\(^1\). However, much like the DPR itself, the decree does not indicate how parental consent can be obtained. For this reason, many websites in Spain have decided to restrict access to children under this age, by putting in place age gating mechanisms – an unintended consequence of the law which is by no means a silver bullet solution.

Outside of the regulatory sphere, many operators have voluntarily implemented age-verification mechanisms and some require a form of parental consent, voluntarily applying COPPA rules to their EU websites.

For example, in order to register a new user on the children’s section of the McDonalds website in Europe – McHappy Studio\(^2\), users are required to give their parents’ email address. Once the email address has been entered, the user is requested to ask his/her parents to check his/her emails and to accept the registration in order to start playing.

---

\(^1\) **Kingdom of Spain**, Royal Decree 1720/2007 of 21 December approving the Regulations implementing Law 15/1999 on the Protection of Personal Data, §13.1: “(...) En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores”.

\(^2\) See [http://www.happystudio.com/](http://www.happystudio.com/), last accessed on 26 September 2013
This type of consent mechanism would probably not be considered valid under the DPR, since it is unlikely to satisfy the “verifiability” requirement.

Prince de LU (Belgium) – age gating

As another case study, we selected “LU Prince” Belgium.

In order to access the LU Prince website, users must respond to a question about their age. While this website does check whether the user is under or over 12 years old, this age verification practice is easily falsifiable by just a click. This practice would not be acceptable in the US where age-screening must not be leading, and is not permitted in child-directed sites because visitors are assumed to be under the age of 13.

Although the examples above suggest that websites have already taken steps to protect children online, the DPR would significantly change the way operators seek to obtain parental consent. In order to provide best-guidance solutions on how to obtain consent in a meaningful and efficient way, the current global legislative landscape on data protection will be analysed.

---


22 *Id.*
III. Global legislative landscape on data protection of children

Very few countries in the world enforce special data protection rules for minors or children.

1. Europe

Currently, rules on children’s data privacy differ across Europe, with authorities providing “rules of thumb” as to what would constitute a safe legal age for data protection related parental consent.

In Spain, the Royal Decree (1720/2007 implementing Law 15/1999 on Data Protection) requires verifiable parental consent to process data for children under 14. Consent can be obtained by providing ID information by parents.

In the UK, the Guidance published by the Data Protection Authority states that parental consent is usually required to collect data from children under the age of 12.

The French Data Protection Agency (CNIL) requires parental consent for the collection of minors’ data. In the context of newsletter subscriptions, only email addresses and the age of a minor can be collected. Other collection of data, including the use of a minor’s image and transfer of a minor’s data obtained through games to third parties is considered illegal.

In Denmark and Sweden, the rule of thumb is that data cannot be collected from children under the age of 15. Germany requires parental consent for children under 14 years old, while Belgium has set the age limit at 12.

In Austria, there are no legal restrictions or case law, although the age of 14 is usually taken as the cut-off point below which consent is required, except for the processing of sensitive data, for which parental consent is required for all minors. Generally, the Data Protection Authorities do not prescribe mechanisms on how to obtain consent, and as such they vary to a large degree.

In the European Union, the DPR also envisages treating sensitive data as a separate category. Article 9 provides that the “the processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health (...) shall be prohibited.”

2. Asian-Pacific Region

Most Asian-Pacific (APAC) countries that have implemented laws or guidelines for online data protection make no reference to children and do not include provisions to obtain parental consent in order to protect children online. There is some debate on the issue of protecting children online currently under way in countries such as Taiwan or Malaysia.

---

23 Kingdom of Spain, op.cit. §13.1
24 UK Information Commissioner’s Office (2010), Personal information online code of practice, available online at: http://www.ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/personal_information_online_cop.ashx, last accessed on 26 September 2013
26 Id.
27 Id.
28 EU Commission (2012), op.cit., §9.1
The South Korean Personal Information Protection Act (PIPA) requires consent from legal representatives for a child under the age of 14. Specifically, “the personal information processor shall, when it is required to obtain the consent in accordance with this Act so as to process the personal information of minors of age below 14, obtain the consent from their legal representatives.”

The Enforcement Decree also specifies that consent can be obtained through various methods, such as email, telephone or via internet.

In Australia, guidelines developed in 2001 to provide additional information on the National Privacy Principles (NPPs) state that “as a general principle, a young person is able to give consent when he or she has sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person; for example if the child is very young or lacks the maturity of understanding to do so themselves.”

However, the 2012 Privacy Amendment Act makes no specific references to the protection of the privacy of children. There is no structure in the Privacy Act or its subsequent amendments for making decisions on behalf of an individual unable to make a decision concerning the privacy of his or her personal information. It is assumed that parents are responsible for making decisions on behalf of children or young people incapable of making the decision themselves.

The Data Protection Commission of Singapore is currently looking into including data protection regulation addressing the right of children.

In Taiwan there have been discussions related to a draft Children Online Privacy Protection Act proposed in 2010. However, no advancements on the issue have been reported since.

3. North America

In Canada, the Consumer Protection Act of Quebec bans commercial advertising directed at persons under the age of 13. According to the Consumer Protection Office, the rule applies to websites as well. Additionally, a Supreme Court decision from 2012 has recognised the “inherent vulnerability of children” and has held that “this results in protection for young people’s privacy”. However, no specific methods to obtain parental consent are prescribed, despite the fact that the federal data protection legislation (Personal Information Protection and Electronic Documents Act – PIPEDA) and its regional counterparts require that consent be obtained for the collection, use and disclosure of personal information.

---

29 Korea (2011) Enforcement Decree of the Personal Information Protection Act, available online at: http://koreanlii.or.kr/w/images/d/d7/DPAAct_EnforceDecree.pdf, last accessed on 26 September 2013
32 Québec (1983), Consumer Protection Act of Quebec, available online at: http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=P_40_1/P40_1_A.html, last accessed on 26 September 2013
personal information.\textsuperscript{35} Obtaining parental consent is complicated by the fact that the collection of birth dates is discouraged by privacy advocates.

To date, the most comprehensive legislation on the protection of children online remains the Children’s Online Privacy Protection Act in the United States.

3.1 The US Children’s Online Privacy Protection Act (COPPA)

After the commercialisation of the Internet in 1995, the Federal Government became increasingly concerned with ensuring privacy protection for data collected in the online environment in light of rapid technological developments.

In 1996, the Children’s Advertising Review Unit (CARU) of the Council of Better Business Bureaus (CBBB) released self-regulatory principles to govern children’s privacy. These essential principles served as the basis of the Federal Government’s Children’s Online Privacy Protection Act (COPPA) adopted two years later.

In the same year, consumer watchdog the Center for Media Education denounced the website KidsCom.com on the grounds of unfair and deceptive practices in their data collection practices.\textsuperscript{36} In the 1997 ruling on the case, the Federal Trade Commission (FTC) publically announced its guidelines concerning data collection from children on the internet. Then, during the 1998 Senate hearings on Internet privacy\textsuperscript{37}, children were particularly singled out as a vulnerable group.

When COPPA was initially enacted, it received widespread support from a variety of stakeholders. The legislation recognised that the most significant risk to children’s privacy involved the disclosure of personal information in arenas where children might be vulnerable to child predators. It created a “sliding scale” of parental consent under which one method, the so-called “e-mail plus”, was permitted in instances involving interaction of a child and a brand so long as no third-party sharing was involved.

The FTC was entrusted to enact rules to administer the act, which finally became effective in April 2000. COPPA has a dual mandate:

1. to protect the privacy of children under the age of 13 in the online environment, and;
2. to get parents more involved and in control with respect to what type of information their children share on the Internet.

COPPA applies to operators of commercial websites who manage services that directly target children and which collect, use or disclose personal information. As such ‘personal information’ means individually identifiable information about an individual collected online, including:

- A first and last name;

\textsuperscript{35} Id.
• A home or other physical address including street name and a city or town;
• An email address;
• A telephone number;
• A Social Security number;
• A persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information;
• Information concerning the child or the parents of that child that the operator collects online from the child and combines with another identifier described above.

The first COPPA Rule defines what factors will be used to determine if a website is directed to children:

• The subject matter;
• Visual or audio content;
• The age of models on the site;
• The language;
• Whether advertising on the website is directed to children;
• Information regarding the age of the actual or intended audience;
• Whether a site uses animated characters or other child-oriented features.

Obtaining parental consent means “making reasonable effort (taking into consideration available technology)” to ensure that parental consent is given before collecting personal information from a child. According to 1998 COPPA, consent is mandatory in most circumstances in which children’s personal data is collected, but the rule recognises a number of important exceptions where interactions may occur between a website and a child without prior parental consent, examined below.

How is consent provided?

Depending on the type of information collected and on the intended use of that information, several proposed methods to obtain parental consent are included in a non-exhaustive list, which will be detailed and analysed in a section further down.

A. If the personal information of the child will be disclosed to third parties, or made publically available, a more robust and reliable method of consent must be used, from the following options:

• Provide a form for the parent to print, fill out, sign, and mail or fax (the “print-and-send” method);
• Require the parent to use a credit card in connection with a transaction (which could consist of a membership or subscription fee, a purchase, or a charge to cover the cost of processing the credit card);

• Maintain a toll-free telephone number staffed by trained personnel for parents to call in their consent; or
• Obtain consent through an email from the parent, if that email contains a digital signature, or other digital certificate that uses public key technology obtained through one of the above methods.

B. If the child’s information is only used for internal purposes, any of the abovementioned methods can be used. Alternatively the “email plus” mechanism may be used, which allows for parental consent to be obtained via email as long as it is coupled with an additional step (the “plus” element of the “email plus” mechanism factor). In this scenario, a screen or user name (aka “pseudonymous data”) is considered personal information when it functions in the same manner as online contact information. This includes any “substantially similar identifier that permits direct contact with a person online.”

3.2 COPPA 2.0

In 2010, concerned about the use of Online Behavioural Advertising (OBA), the FTC announced plans to review COPPA ahead of the initial 2015 plans, citing “(…) rapidly evolving technology and changes in the way children use and access the Internet”\(^41\). When COPPA was first enforced more than 10 years ago, the variety of online services and social networks, as well as the extent to which children use the internet, were trends which could not have been anticipated. According to Common Sense Media research conducted in the United States, more than 22% of children aged five to eight surf the Internet at least once a day, while 44% say they go online at least once a week.\(^42\)

In particular, the FTC looked at whether to expand definitions of “child” and “personal information” to reflect technological advancements, whether current exclusions for activities constituting “support for the internal operations of a website” were adequate, and whether to update the existing methods of obtaining parental consent.

Definition of “child”

The Act defines a “child” as any individual that is younger than 13. This cut off age was never fully explained by legislators, although during Senate Committee hearings on Children’s Online Privacy, Senator Richard Byron argued that “children under the age of 12 (…) are not likely to have the judgment to know what is appropriate [when disclosing personal and private information on the Internet]". In the course of 2012, some stakeholders proposed to increase the definition up to the age of 18 years old, in order to extend parental consent requirements to the 13-17 age group, in an attempt to ensure privacy protection for adolescents as well. This idea was not taken into account since the FTC has no legal authority to change the age and because it raised constitutionality.


\(^42\) Id.

\(^43\) US Senate Communications Subcommittee Hearing on Children’s Online Privacy Bill, op.cit.
problems, as some commentators argued\textsuperscript{44} that it would limit free speech, and thus breach the first amendment.

Furthermore, it was argued that by raising the age limit to also include adolescents, privacy would actually be reduced in practice, because more information (e.g. credit card information) would have to be collected to avoid age frauds.

**Definition of “personal information”**

One of the main objectives of the COPPA review was to examine the definition of “personal information” to see if it was consistent with the pace of technological developments. The FTC started the process with the idea that IP addresses and other device identifiers should be included in the definition in order to address Online Behavioural Advertising. Another objective was to include apps in the definition of a website or online service. Children today access the internet from a larger variety of devices, the FTC argued, and the rules that applied 15 years ago are no longer sufficient to protect the privacy of children. As such, the definition of personal information has been expanded to also include:

- A screen name (where it is similar to online contact information, e.g. an e-mail used as a screen name but excluding anonymous usernames and passwords);
- A photograph, video, or audio file where such file contains a child’s image or voice;
- Geolocation data sufficient to identify a street name or the name of a city or town; or
- Persistent identifiers that can be used to recognise a user over time or across different locations, such as cookies, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier.

However, the definition of “personal information” excludes a zip code.

<table>
<thead>
<tr>
<th>Children's Online Privacy Protection Act 1998</th>
<th>Children's Online Privacy Protection Act 2012</th>
</tr>
</thead>
</table>
| individually identifiable information about an individual collected online, including—  
(A) a first and last name;  
(B) a home or other physical address including street name and name of a city or town;  
(C) an e-mail address;  
(D) a telephone number;  
(E) a Social Security number;  
(F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or  
(G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph. | individually identifiable information about an individual collected online, including:  
(a) A first and last name;  
(b) A home or other physical address including street name and name of a city or town;  
(c) Online contact information as defined in this section;  
(d) A screen or user name where it functions in the same manner as online contact information, as defined in this section;  
(e) A telephone number;  
(f) A Social Security number;  
(g) A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifier includes, but is not limited to, a customer |

number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;  
(h) A photograph, video, or audio file where such file contains a child’s image or voice;  
(i) Geolocation information sufficient to identify street name and name of a city or town; or  
(j) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

The inclusion of persistent identifiers in the definition of personal information – except when these are used to support the “internal operations of the website” - has been heavily criticised by the industry. The Toy Industry Association, Yahoo! and the American Association of Advertising Agencies have argued that such information cannot locate an individual, but rather a device and that it will consequently affect behavioural advertising on any website that cannot prove it is not child oriented.

They also argued that defining persistent identifiers as personal information in all circumstances would basically amount to the end of all child-directed services offered by both large and small businesses, or force them to severely limit the functionalities or inter-activeness offered to children.

In addition, without the ability to analyse traffic, offer some personalisation, maintain security, and use information in other ways necessary to support the business, child-oriented digital content simply will not be offered. Conversely, consumer organisations, such as the Centre on Law & Information Policy, have applauded the revised definition, arguing that present-day technology makes individuals easily identifiable if this information is combined.

**Definition of “website directed to children”**

With the revision of the Act, the definition of website directed to children was also reviewed and several criteria were considered – the subject matter, the visual content, the use of animated characters or child celebrities, the music or other audio content, the age of the models pictured on the website, the language used and the type of advertising. The FTC has also expanded COPPA to cover websites “secondarily” targeted to children, an interpretation that may prove quite problematic for teen-directed sites.

---

48 Comments of the Centre on Law & Information Policy on COPPA (comment 18) (2011) available online at: [http://www.ftc.gov/os/comments/copparulereview2011/00320-82235.pdf](http://www.ftc.gov/os/comments/copparulereview2011/00320-82235.pdf), last accessed on 26 September 2013
49 Federal trade Commission, op.cit., § 312.2: Definitions - Website or online service directed to children
<table>
<thead>
<tr>
<th>1998</th>
</tr>
</thead>
<tbody>
<tr>
<td>A website shall be considered as directed to children if:</td>
</tr>
<tr>
<td>(i) It targets children</td>
</tr>
<tr>
<td>(ii) that portion of a website or online service that is targeted to children</td>
</tr>
<tr>
<td>LIMITATION—A website shall not be deemed directed to children solely for referring or linking to a website or online service directed to children.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Means a commercial website or online service, or portion thereof that is targeted to children.</td>
</tr>
<tr>
<td>(a) Criteria: subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language, as well as whether advertising promoting or appearing on the website or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.</td>
</tr>
<tr>
<td>(b) A website or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users.</td>
</tr>
<tr>
<td>(c) A website or online service that does not target children as its primary audience, shall not be deemed directed to children if it:</td>
</tr>
<tr>
<td>(i) does not collect personal information from any visitor prior to collecting age information;</td>
</tr>
<tr>
<td>(ii) prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part.</td>
</tr>
<tr>
<td>(d) A website or online service shall not be deemed directed to children solely because it refers or links to a website or online service directed to children.</td>
</tr>
</tbody>
</table>

Many industry stakeholders expressed negative comments, arguing that expanding the definition of “website directed to children” to also include websites not primarily addressed to children went beyond the scope of COPPA. This would impose unnecessary operational and financial costs on the industry, they said. Furthermore, stakeholders argued that the proposed definition would stifle innovation and the design of child appropriate websites, thus effectively paving the way for children to go to websites which do not have adequate content.
Major failings of COPPA

The process that led to the review of COPPA was the opportunity for many actors to underline some of the legislation’s major weaknesses:

- **Difficult to enforce**: Due to the lack of cost-effective methods for obtaining parental consent, very few sites are willing to create useful internet services for children. The direct consequence is that children learn early in their youth how to lie about their age online. Research\(^5\) found that parents teach children to lie about their age to circumvent age limitations. US academics surveyed a national sample of parents and guardians with children aged 10–14 living with them and found that a third (36%) of all parents surveyed reported that their child joined Facebook before the age of 13, and two-thirds of them (68%) admitted helping their child to create the account. There is also no data about how often parents use the means of notice and consent COPPA provides, casting doubts about its popularity and efficiency. As a result, most child-directed websites operate under one of the exceptions to COPPA that allows a one-time use, multiple online contact with simply a notice to a parent, or e-mail plus.

- **COPPA restricts children’ access to online material**: Since banning users under the age of 13 to access a website is perceived by some website operators as easier and more cost-effective than attempting to comply with COPPA, the Act prevents children from fully benefiting from the online content available. By focusing too much on the danger linked to technology and the internet, regulators forget the opportunity that they also represent and prevent children from making the most of their online experience.

- **Disproportionate attention on first parties**: Additionally, regulators should focus on the risks children face when exposing data to third parties through social media rather than on the risks of children being targeted by advertisers.

- **Excessive focus on the collection of data, not on its processing**: Commentators have cautioned against focusing solely on the collection of information and have suggested focusing also on how information is used once it is collected. Both aspects are important. By placing too much emphasis on consent at collection, regulators may get the impression they have addressed parental and societal concerns, but in fact they fail to effectively protect children once they have received (or bypassed) their parent’s consent and begin interacting with content providers.

- **Business costs**: Since website operators do not have a reliable way to obtain parental consent online, COPPA-compliant websites are forced to adopt costly offline consent verification methods which imply technical investment as well as human intervention. This is particularly detrimental to small businesses.

---

which might not have the financial and human resources required. Without clear understanding of what the exception for support for internal operations means across the ecosystem, the complexity of the updated Act will add further cost burden to small businesses as it will force them to seek lawyers’ expertise to make sure their activities comply with the new rules. The inclusion of persistent identifiers to the list of what qualifies as personal information (unless processed to support the internal operations of a website or service) has consequences beyond the content created or originated on a website or online service. Persistent identifiers should be assessed and fully controlled by website operators.

Notably, the Walt Disney Company\(^{51}\) argued that sites targeted at both children and adults, such as its own online service, should be allowed to distinguish among users. Disney proposed a refined approach to the definition of websites targeting children, including a classification scheme adding a separate category - “family-friendly” websites. As these websites target both adults and children, distinct privacy rules should therefore apply. “Family friendly websites” would have to satisfy more robust privacy rules than general audience websites, extended to all users. Specifically, Disney proposed several rules that “family friendly” websites would have to comply with:

- Verify age before collecting personal information and obtain parental consent if the user is under 13
- Take reasonable measures to prevent the disclosure of personal information, unless the operator has actual knowledge that the user is an adult
- When the operator has actual knowledge that the user is a child it will not passively track him or her, or collect precise geolocation information without prior parental consent\(^{52}\).

This contribution from Disney sparked a revision of the COPPA text to reflect the fact that websites which target children and adults simultaneously fall under a different category (see table above, paragraph c).\(^{53}\) In practice, many websites already use age verification techniques before collecting personal information; but may not age-screen at sites or areas primarily directed to children under 13, as they must operate under an assumption that all visitors are under 13.

\(^{51}\) Comment of the Walt Disney Company on COPPA (comment 170) (2011) available online at: http://www.ftc.gov/os/comments/copparulereview2011/00368-82393.pdf, last accessed on 26 September 2013

\(^{52}\) Id.

\(^{53}\) Federal Trade Commission, op.cit., § 312.2: Definitions - Website or online service directed to children
How to obtain parental consent?

The COPPA Rule states that an operator must make “reasonable efforts (taking into consideration available technology)” to ensure that before collecting personal information from a child the parent consents to the collection, use and/or disclosure of such information.

Websites have two obligations to fulfill. The parent must be directly notified about the intention to collect personal data from their child, and a privacy policy should be posted online in such a manner that it is clearly visible and easily accessible. The direct notice should include a notification that the operator has collected personal information from the child, clearly state that the parent’s consent is required, what (if any other) personal information the operator intends to collect, a hyperlink to the operator’s online notice, what method to obtain parental consent will be used and a mention that if consent is not provided in reasonable time, the parent’s online information will be deleted from records.

There are several approved methods to obtain parental consent, some of which are detailed below. Importantly, the list is non-exhaustive and the FTC allows websites to use other approval methods. The revision process revealed that most website operators did not use or develop other methods besides the ones already specified by COPPA, for which reason in the 2012 review, an amendment allowing operators to seek approval for voluntarily developed methods of consent was included. According to the Rule, “an interested party may file a written request for Commission approval for parental consent methods not currently enumerated”.

<table>
<thead>
<tr>
<th>Children’s Online Privacy Protection Act 1998</th>
<th>Children’s Online Privacy Protection Act 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile;</td>
<td>Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;</td>
</tr>
<tr>
<td>Requiring a parent to use a credit card in connection with a transaction;</td>
<td>Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;</td>
</tr>
<tr>
<td>Having a parent call a toll-free telephone number staffed by trained personnel;</td>
<td>Having a parent call a toll-free telephone number staffed by trained personnel;</td>
</tr>
<tr>
<td>Using a digital certificate that uses public key technology;</td>
<td>Having a parent connect to trained personnel via video-conference</td>
</tr>
<tr>
<td>Using e-mail accompanied by a PIN or password obtained through one of the verification methods listed in this paragraph</td>
<td>Verifying a parent’s identity by checking a form of government issued identification against databases of such information, where the parent’s identification is deleted by the operator from its records promptly after such verification is complete.</td>
</tr>
<tr>
<td><strong>“Sliding Scale/E-mail Plus Method”</strong> Provided that: for the period until April 21, 2002, methods to obtain verifiable parental consent for uses of information may also include use of e-mail coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include:</td>
<td><strong>“Sliding Scale/E-mail Plus Method”</strong> Provided that, an operator that does not “disclose” children’s personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: sending a confirmatory email to the parent following receipt of consent, or</td>
</tr>
</tbody>
</table>

---

54 Id.
55 Ibid., Part 312, pp.81 - 82
56 Ibid., Part 312, §312.12(a): Voluntary Commission Approval Process
<table>
<thead>
<tr>
<th>Children’s Online Privacy Protection Act 1998</th>
<th>Children’s Online Privacy Protection Act 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>sending a confirmatory e-mail to the parent following receipt of consent; or obtaining a postal address or telephone number from the parent and confirming the parent’s consent by letter or telephone call.</td>
<td>obtaining a postal address or telephone number from the parent and confirming the parent’s consent by letter or telephone call.</td>
</tr>
<tr>
<td>Safe Harbors were implemented since the 1998 Rule; however, safe harbour programs were not initially included in the approved methods list.</td>
<td>Safe harbor approval of parental consent methods. A safe harbor program approved by the Commission may approve its member operators’ use of a parental consent method not currently where the safe harbor program determines that such parental consent method meets the requirements (COPPA).</td>
</tr>
</tbody>
</table>

a. **Print and Sign**

This method requires parents to physically sign a consent form and then return it by post mail, fax or electronic scan to the website operator. The ‘print and sign’ method has been criticised for being too costly and time inefficient. Estimates suggest it costs roughly $3 per child to obtain a signed parental consent form. Industry commentators\(^{57}\) provided their support especially for the electronic scan method, as it is more cost/time efficient.

b. **Credit card information and alternative online payment systems**

In the 2011 initiated review, the FTC proposed to extend the type of payment information that a parent could provide. Importantly, the FTC clarified that using credit cards to give parental consent should be limited to situations that involve actual monetary transactions\(^{58}\). The Commission also concluded that debit card information and online payment systems qualify as stringent methods of providing parental consent when monetary transactions are involved.

eBay\(^{59}\) suggested implementing a system which is similar to PayPal that requires financial control for age verification, given that persons under the age of 18 cannot apply for an individual bank account. The suggested programme would allow the primary account holder – the parent – the possibility to set sub-accounts for the child(ren) that could then allow them to place limits on their child’s online activity. eBay also proposed to expand the abovementioned programme into a platform where parents can provide permission for their children to access multiple websites.

c. **Government issued identification**

This is one of the most controversial approved consent methods. The FTC was motivated in its decision to recognize this method on the grounds that it is one of the most trustworthy means of ensuring that the person providing consent is actually the parent. It also emphasized the fact the collection of such information should be limited only to segments needed to verify the data.\(^{60}\) While

---

\(^{57}\) *Comment of Yahoo! (comment 180), Direct Marketing Association (comment 37) and of kidsSAFE Seal Program by Samet Privacy (comment 81) on COPPA available online at: [http://www.ftc.gov/os/comments/copparulereview2011/](http://www.ftc.gov/os/comments/copparulereview2011/), last accessed on 26 September 2013*

\(^{58}\) *Federal Trade Commission, op.cit., Part 312, pp. 66-67*

\(^{59}\) *Comment of eBay on COPPA (comment 40) (2011), available online at: [http://www.ftc.gov/os/comments/copparulereview2011/00328-82251.pdf](http://www.ftc.gov/os/comments/copparulereview2011/00328-82251.pdf), last accessed on 26 September 2013*

\(^{60}\) *Federal Trade Commission, op.cit., Part 312, p.64*
some websites already use this mechanism (e.g. Facebook\textsuperscript{61}), many opine that collecting such sensitive information poses high privacy risks\textsuperscript{62}. Intel\textsuperscript{63} and the Marketing Research Association\textsuperscript{64} cautioned that this method may send a confusing message to the industry by encouraging them to use sensitive information, and advising them to minimise data collection at the same time. Others, such as the New York Intellectual Property Law Association, argued\textsuperscript{65} that this method had strong privacy implications, and that parents’ data should not be put at risk for the sake of protecting their children’s data. Moreover, most parents would not share this type of sensitive data simply to allow a child to play games online.

d. “Sliding Scale”/ “E-mail Plus”

This method can be used when a website or online service is collecting children’s personal information for internal use only. In this case the operator can obtain parental consent by sending an email to the parent. In the case operators wish to collect additional information or share it with a third party, an additional step will be required, such as a printed form or videoconference. The FTC initially introduced this as a temporary method, recognising that it was not a reliable method of verifying parental consent. However, due to the wide appeal it enjoys in the industry, the Commission agreed in 2007 to grant the sliding scale permanent status for the foreseeable future.

Many website operators credit the simplicity of the sliding scale approach as well as its relatively low operational costs, compared to other methods. For example, the Association of Educational Publishers\textsuperscript{66} argued that the method strikes the right balance between getting parents involved and giving children online freedom, while the Toy Industry Association argued\textsuperscript{67} that, while the sliding scale is not perfect, other more efficient technologies have not yet been developed. The NGO TechFreedom\textsuperscript{68} mentioned that eliminating this method would put unnecessary burdens on small operators. Finally, Wired Trust argued\textsuperscript{69} that eliminating the sliding scale would hamper innovation.

Detractors argue that the method is easily falsifiable because there is no way to ensure that the person providing consent is actually the parent. One commentator noted that “trying to stop pre-teens from using the Web is like trying to nail Jell-O on the wall... Each of them have a sister, a brother, a friend who has legit[imate] access. As is the case with all adult material, pre-teens can find it.”\textsuperscript{70}

\textsuperscript{61} Comments of Facebook on COPPA (comment 50) (2011): “This approach achieves the delicate balance of making it easy for the parent to provide consent, while making it difficult for the child to pose as the parent.”, available online at: http://www.ftc.gov/os/comments/copparulereview2011/00369-82394.pdf, last accessed on 26 September 2013

\textsuperscript{62} See for example TechFreedom, New York Intellectual Property Law Association

\textsuperscript{63} Comments of Intel Corporation on COPPA (comment 72) (2011), available online at: http://www.ftc.gov/os/comments/copparulereview2011/00278-82142.pdf, last accessed on 26 September 2013

\textsuperscript{64} Comments of the Marketing Research Association on COPPA (comment 97) (2011) available online at: http://www.ftc.gov/os/comments/copparulereview2011/00301-82205.pdf, last accessed on 26 September 2013

\textsuperscript{65} Comments of New York Intellectual Property Law Association on COPPA (comment 117) (2011) available online at http://www.ftc.gov/os/comments/copparulereview2011/00364.html, last accessed on 26 September 2013

\textsuperscript{66} Comments of the Association of Educational Publishers on COPPA (comment 7) (2011), available online at: http://www.ftc.gov/os/comments/copparulereview2011/00048-81886.pdf, last accessed on 26 September 2013

\textsuperscript{67} Comments of the Toy Industry Association on COPPA, op.cit.

\textsuperscript{68} Comments of TechFreedom on COPPA (comment 159) (2011) available online at: http://www.ftc.gov/os/comments/copparulereview2011/00375-82401.pdf, last accessed on 26 September 2013

\textsuperscript{69} Comments of Wired Trust on COPPA (comment 177) (2011) available online at: http://www.ftc.gov/os/comments/copparulereview2011/00377-82403.pdf, last accessed on 26 September 2013

\textsuperscript{70} Joshua Warmund, op.cit., p.208
Ultimately, however, the FTC agreed to continue to authorize this method of parental consent. It appears that they were convinced that operational difficulties and costs of other methods of consent, given the relatively low privacy risks of purely internal marketing, weighed in favour of continuation.

e. “Safe-harbour” programmes

COPPA terms allow companies to follow the “safe harbour” provision, which was specifically designed to encourage industry self-regulation. Article 312.11 on safe harbour programmes of the COPPA rule states that:

“Industry groups or other persons may apply to the Commission for approval of self-regulatory program guidelines (“safe harbor programs”). The application shall be filed with the Commission’s Office of the Secretary. The Commission will publish in the FEDERAL REGISTER a document seeking public comment on the application. The Commission shall issue a written determination within 180 days of the filing of the application.”\(^{71}\)

The 2012 review of the COPPA brought about increased FTC control over safe-harbour programmes. Consequently, FTC-approved safe harbours must submit annual review reports and are required to store data on consumer complaints alleging violation of guidelines, records of disciplinary actions taken against the websites, and results of an independent assessment on compliance for a 3-year period. The initial proposal also required keeping on record the names of companies in breach of the guidelines. However, following comments from stakeholders, this proposal was not included in the final text.

There are currently four FTC approved safe-harbour programmes implemented by: Children’s Advertising Review Unit (CARU) of the Council of Better Business Bureaus (CBBB), PRIVO, TRUSTEe and Entertainment Software Rating Board (ESRB).

Most US firms do not participate in these programmes as CARU reviews and initiates self-regulatory action for any website that it believes falls under CARU’s jurisdiction, regardless of whether the firm participates in its safe harbour programme.

Still, the rules enforced by the safe-harbour programmes, similar to COPPA rules, are worth mentioning. These programmes aim to ensure that the operators joining their programme apply a streamlined, verified process, giving the industry the option to comply with COPPA at lower costs and with fewer risks. Additionally, website operators joining safe-harbour are first subject to the disciplinary procedures of the safe-harbour programmes rather than the FTC.

**Voluntary Submission of New Parental Consents Mechanisms**

An amendment was introduced in the 2012 revision with the aim of encouraging industry innovation in relation to parental consent mechanisms. The FTC specified even in the first COPPA Rule that the list of parental consent methods was non-exhaustive and that website operators were encouraged to develop newer, more efficient methods. However, by 2012 it had become clear that both safe harbour programmes and other operators were vastly implementing only the methods specified by

\(^{71}\) Federal trade Commission, *op.cit.*, Part 312, §312.11
COPPA and that newer methods were not being developed. As such, the revised COPPA Rule contains an amendment laying down the requirements and procedures to obtain approval for self-developed methods to obtain parental consent:

“Voluntary Commission Approval Process:
(a) Parental Consent methods. An interested party may file a written request for Commission approval of parental consent methods not currently enumerated (...). To be considered for approval, a party must provide a detailed description of the proposed parental consent methods, together with an analysis of how the methods meet [the requirements]. (...) The Commission shall issue a written determination within 120 days of the filing of the request;”

g. Proposed methods rejected by the FTC
Two other mechanisms were considered and rejected by the FTC: digital/electronic signatures and creating platform methods enabling parents to provide consent for multiple websites at a time. Digital signatures were struck down on the grounds that they still remain an easily falsifiable mechanism, although scanned consent forms are acceptable.

Several stakeholders proposed solutions to develop a ‘multiple-consent’ platform, as a way to ease operator burdens. Consequently, benefits would have included the development of interactive educational content for children and increased privacy by avoiding the collection of personal data by several websites. For example, Disney envisaged\(^{73}\) two such platforms: a “Kids Privacy Portal” through which parents could express privacy preferences for multiple websites at a time. This solution would particularly simplify consent mechanisms for operators that hold multiple websites. The FTC rejected the idea of out-rightly including ‘multiple-consent’ platforms in the rule, specifying that the rules as such do not exclude the possibility of developing this kind of technology.

Exceptions
The Act also provides for exceptional cases in which it is not necessary to gain parental consent before collecting limited pieces of information from children. This creates a flexible and workable framework that does not excessively burden website operators.

- IP addresses and other persistent identifiers can be used without parental consent if the purpose of collecting information is to protect the “security and integrity” of the website or online service.
- The Rule allows that websites collect the name or email address of a child and of a parent in order to be able to obtain consent;
- Website operators may also collect parents’ online information if the purpose is to “voluntarily” inform and update them about the child’s participation on a website.
- COPPA allows for what is known as “the one-time-use exception”: websites can collect online contact information from a child without requesting parental consent with the purpose of responding to a one time specific request from a child, like sending them a forgotten password;

\(^{73}\) Comments of Disney on COPPA, op.cit.
• The “multiple-uses” exception provides that an online service may collect online contact information from a child and his or her parents in order to respond directly to multiple requests from the child. In this case, the service provider must “make reasonable efforts, taking into account available technology” to obtain parental consent;
• “Child Safety Exception”: No prior consent is required if the information is provided to protect the safety of the child, and if the information is not used or disclosed for any other purpose;

The 2012 Revision brought about the introduction of two new exceptions which reflect technological developments in the online environment and bring consistency with the amendments made to the Act:

• No prior consent is required if data is collected only for internal purposes “where an operator collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the website or online service”;24
• Where an operator covered under paragraph (b) of the definition of website or online service directed to children collects a persistent identifier and no other personal information from a user who affirmatively interacts with the operator and whose previous registration with that operator indicates that such user is not a child.

These two definitions have proved to be a bit confusing and their implementation is therefore still widely discussed by the industry and the FTC.

24 Federal trade Commission, op.cit., Part 312, § 312.5(g)
IV. COPPA in practice – some examples

In order to better understand how COPPA works, which are the most effective methods of obtaining consent and how the Act has impacted the online world, 41 websites were analysed – including social networks, websites directed to children and websites where only part of their content targets children. What was found is that, in practice, many websites use the sliding scale and only ask for minimal information from children when signing up or avoid collecting personal information altogether. Notably, most of the websites analysed used age-verifying mechanisms, blocking children under the age of 13 from registering for an account or newsletter.

![Parental Consent Methods - Analysis](chart)

*Drop-off rate*

One of the collateral consequences of introducing online mechanisms to obtain parental consent to a website is a potentially significant drop in visitors. A company agreed to share the experience it had when it decided to create an online experience for children by setting up a chat room on their website. As this required the processing of children’s data, and therefore compliance with COPPA, the company set-up a process validating parental consent upon the provision of a passport or a social security number. Following these changes made to the website, the company saw a drop-off rate of visitors of 99%. The company also tested other mechanisms on different websites and saw a 70-75% drop-off rate when they required the validation of parental consent by email and asked parents to sign up/create ID account, with an additional 15% drop-off during the actual creation of an account.
Different methods used to obtain parental consent

Eight of the websites consulted made use of the sliding scale method.

**PBS Kids**

PBS Kids\(^{75}\), one of the most popular children’s online platforms and TV channels, does not collect any personal information from a child if he/she wishes to create a virtual identity; however, if he/she wants to submit a comment or a letter, PBS collects their first name and the age.

**The Club Penguin**

The Club Penguin\(^{76}\), part of the Disney franchise, requests the parent’s e-mail address to which it sends a notification.

If the child gives the correct email of his/her parent, the parent receives a message with an activation code and information about the Club Penguin and children’s online privacy.

---

\(^{75}\) See [http://pbskids.org/](http://pbskids.org/), last accessed on 26 September 2013

\(^{76}\) See [http://play.clubpenguin.com/#/create/](http://play.clubpenguin.com/#/create/), last accessed on 26 September 2013
Only a few of the websites analysed used alternative methods of obtaining parental consent.

**Neopets** – a platform where children can raise virtual pets and **RateMyDrawings** – a platform where children can draw and then upload their work, require parents to download, print and sign a parental consent form.

**Sweety High**, a platform designed for teenage girls, offers several options to obtain parental consent when a child under 13 wants to sign up.

Parents can give consent via email, provide the last four digits of their Social Security Number (SSN), sign and fax a printed consent form, or provide their credit card information.

---

77 See [http://www.neopets.com/signup/index.phtml](http://www.neopets.com/signup/index.phtml), last accessed on 26 September 2013

78 See [http://www.ratemydrawings.com/community/register.php](http://www.ratemydrawings.com/community/register.php), last accessed on 26 September 2013

79 See [https://www.sweetyhigh.com/](https://www.sweetyhigh.com/), last accessed on 26 September 2013
Some websites directed to children now only offer paid membership. This method offers greater guarantee that the parent is actually involved in the decision-making process and that he/she has stricter control over the type of information the child accesses, because consent is associated with the use of a credit card in connection with a transaction. Parents can pay the membership fee either by credit card or by using alternative payment systems such as PayPal. Membership fees cover the administration costs that COPPA implies, that other commercial-oriented websites cover through advertising. In 2005, the estimated cost per child for obtaining verifiable parental consent was US$45, considering that many child-oriented websites rely heavily on constant human moderation and oversight.

Moshi Monsters—an online game where children can raise virtual pets or Animal Jam uses this type of parental consent mechanism.

No examples of websites offering the possibility to obtain parental consent via video-conference or by toll-free telephone calls were found. These methods are not only burdensome from a human resource and financial perspective, but are also more time-costly, which would explain their lack of popularity.

The sliding scale appears to be the preferred method of the industry and is widely used because websites frequently collect information simply for internal marketing purposes. As pointed out by many COPPA commentators, email consent is the least expensive, most time efficient and most easily understandable method available to engage parents in their children’s online activities. On the down side, the fact that this method is easy to use and to understand by all sides makes it easily falsifiable and also hampers innovation and the development of newer, more effective methods. As argued by think-tank TechLiberation: “a great number of sites and services that live under COPPA

81 See http://www.moshimonsters.com/affiliate/google_global?clid=CK7-qNTWrYCFabLsAod0HEAQ, last accessed 19 March 2013
82 See https://www.animaljam.com/membership, last accessed on 26 September 2013
use this method to stay in compliance with the law. This pulls the rug out from under them and creates major short-term marketplace uncertainty.\textsuperscript{83}

**Cartoon Network**\textsuperscript{84}, a popular cartoon channel in the US and an online platform offering games and other activities, advises children to use a nickname when registering. According to COPPA parental consent exceptions, website operators can collect email addresses from children to respond to “one-time” inquiries. Cartoon Network does not store the address in a retrievable form and uses them “to respond to an inquiry from the child on a one-time basis, for example, instances regarding a lost user name or password”.\textsuperscript{85}

\textbf{‘We do not collect personal data from children’}

Other websites directed to children, such as the online game platform **KidsCom.com** (right), avoid collecting any personal information from subscribers\textsuperscript{86}, but rather encourage children to use nicknames. If a password is forgotten, some operators ask to answer to a ‘safety question’, such as “where were you born?” but avoid collecting any identifiable information. The username and the answer to the safety question will then be used to retrieve lost passwords, without requiring the email of the child. Kids.com only offers the option to retrieve passwords for paying subscribers but not for free users, to completely avoid collecting information.


\textsuperscript{84} See [www.cartoonnetwork.com](http://www.cartoonnetwork.com), last accessed on 26 September 2013

\textsuperscript{85} Id.

\textsuperscript{86} See [http://www.my.kidscom.com/jsp_a01_mkc/jsp_a01_b04_mis/jsp_a01_b04_c01_registration/kc_register.jsp](http://www.my.kidscom.com/jsp_a01_mkc/jsp_a01_b04_mis/jsp_a01_b04_c01_registration/kc_register.jsp), last accessed 26 March 2013
Unintended consequences: blocking out children under 13

Many websites that do not only have content directed specifically at children have decided to introduce age-gating mechanisms to block children under 13 instead of implementing mechanisms to obtain parental consent.

For some online businesses, the reason for blocking people under the age of 13 from entering their website because COPPA compliance is expensive. Compliant costs include employing additional staff to design and monitor the online privacy policy statements, hiring attorneys to review the privacy policies, as well as coordinating the collection and securing the storage of parental consent forms.

In 2012, experts estimated that these costs would amount to between 50 cents and three US dollars per child interaction, or up to $US 100,000 per year, for a medium-sized website. In its comments to the FTC, the Toy Industry Association (TIA) said that the costs of compliance with the new Law were underestimated by the FTC. It stated that the FTC estimation – that the total burden of complying accounted for 40,000 hours at a cost of $US 5,240,000 in total (60 hours, affecting 2,000 websites, annualised to 20 hours per year for 3 years) – was grossly understated. Indeed, TIA calculated that this meant that the estimate was based on an assumed labour rate of $US 150 for lawyers and $US 36 for technical personnel, although TIA members typically consult with specialized attorneys who understand children’s privacy and data security laws whose average rates are two to three times the Commission’s estimates. Similarly, engaging expert technical personnel can, on average, again involve hourly costs that are 2 -3 times the Commission’s estimates, TIA wrote.

Some websites decided to disable some features of to avoid collecting any children’s data. For instance, the UK website of "Thomas the Tank Engine" books and toys decided to eliminate their e-mail and chat room features because they could not afford to comply with COPPA.

Facebook and other social networks have been repeatedly criticised for allowing children to create profiles and have, as a consequence declared that these platforms are not intended for children under 13 and have blocked their access.

See http://www.inc.com/encyclopedia/childrens-online-privacy-protection-act-coppa.html; last accessed on 8 July 2013

Comments of the Toy Industry Association on COPPA, op.cit.

See https://www.facebook.com/, last accessed on 26 September 2013
Nevertheless, the practices of social networks have resulted in the FTC expanding the definition of “website directed to children”. This has led even websites that do not primarily address children to introduce age-verification mechanisms in order to avoid being accused of collecting information with “actual knowledge”. Even before COPPA was officially enforced in 2000, some companies decided that the most cost-effective option was to stop communicating with children and to delete all accounts of children under 13.90

Websites such as Disney.com, which is a self-declared “family-friendly”91 website that does not target only children, does not allow children who declare they are younger than 13 years old to sign up for newsletters or emails. This allows Disney to avoid seeking parental consent. The website also uses cookies to remember the IP address and block further attempts of signing up.

In order to register for a free account at zynga.com, a platform for online games for children92, the users must declare that they are 13 years old or older. The website uses cookies, so the age-blocker cannot be avoided by just reloading the page and giving another age.
An age verifying mechanism is also introduced when landing on the official website of mms.com93. Access to the website is denied if the visitor enters an age younger than 13.

A cookie tracks the IP address which prevents a child from trying to circumvent the age verification mechanism by just reloading the page and entering a new date of birth.

93 See http://www.mms.com/, last accessed on 26 September 2013
V. Lessons from COPPA

COPPA was designed to achieve two main goals: (1) to protect the personally identifiable information of children collected online and (2) to enhance parental involvement in their children’s online activities. The framework has been accused of limiting the functionality of children’s websites, creating “walled, closed gardens”, for which parents have to pay admission fees and of having crippled small businesses.\(^\text{94}\)

American media researcher danah boyd cautioned that regulation should be focused on how the information is used, and on what happens when the child is on the website rather than on the gathering of information. We should keep in mind that “children need to play online”\(^\text{95}\) because the Internet offers the opportunity for children to develop their creativity and it should be used as a learning tool.\(^\text{96}\)

Additionally, by extending the definition of “personal information” to also include persistent identifiers, and by also expanding the definition of “data collection”, the result may be that websites directed to children will become even less interactive and that functionalities will be even further limited, especially if common sense exceptions for collection with low/no privacy risks are not recognised. The danger is two-fold: children will not be able to truly benefit from the educational power of the internet and they may also go to general audience websites which do not fall under the scope of COPPA. Legislation designed to protect children online should be enabling and not disruptive.

Moreover, the mechanisms set in place do not help children or parents to understand the importance of online privacy. Privacy policies - posted by websites as a requirement of COPPA - are often not visible and hardly ever read thoroughly, and therefore fail to educate children on the importance of not sharing personal information. As Denise Tayloe noted, one of the unintended consequences of COPPA is that “Children quickly learned to lie about their age in order to gain access to the interactive features on their favourite websites”\(^\text{97}\).

However, COPPA remains a pioneering piece of legislation to provide a valid and workable mechanism to increase the level of children’s privacy online.

1. **Clear criteria defining “websites directed to children”**

COPPA clearly defines what constitutes a “website directed to children” by specifying the criteria to be considered. The Act also clarifies that the rule only applies to websites having “actual knowledge” about collecting information children. Without this specification, websites that have collected personal information from children, because the child has, for example, lied about his or

\(^{94}\) Berin Szoka and Adam Thierer, *op.cit.*

\(^{95}\) Id.


\(^{97}\) See [Denise Tayloe](https://www.privacyassociation.org/publications/2006_10_its_time_to_comply_with_coppa), 1 October 2006, It’s Time to Comply with COPPA, *iapp newsletter*, available online at: [https://www.privacyassociation.org/publications/2006_10_its_time_to_comply_with_coppa](https://www.privacyassociation.org/publications/2006_10_its_time_to_comply_with_coppa), last accessed on 26 September 2013
her age, would also be liable to COPPA infringements. Furthermore, it rightly exempts from the Rule websites that host third party links or applications that collect personal information from children, while the websites themselves do not. This is the case of, for instance, Apple which allows third-parties to sell apps through its website.

2. Non-exhaustive list of parental consent methods and incentives for innovation

COPPA lists several methods to obtain parental consent from which operators can choose. The list is imperfect, and most of the methods have been criticized by the industry or consumer organisations for being too costly, too difficult to implement or requiring sensitive data from parents (such as SSN or credit card information). For example, Joshua Warmund argues that the methods to obtain parental consent proposed by COPPA are “impractical, inadequate and constitutionally suspect” and also fail to “adequately protect the child’s personal information.” The research argues that the new requirements are associated with high implementation costs for operators. Users quickly leave websites that have limited functionalities or when registration processes stand between them and the content. In fact, the parental consent requirements can act as gate-keepers themselves, driving children away from the website to other sites which are more easily accessible. Consequently, this also discourages operators from determining the age of their users.

Importantly, the FTC has specified that the list of methods to obtain consent is ‘non-exhaustive’ and that websites are encouraged to come up with new, more effective solutions. To solidify its intention, the revised COPPA Rule contains a provision on “voluntary parental consent methods” allowing interested parties to submit requests for the approval of new consent methods.

The sliding scale remains the preferred method of both industry and consumers, having been praised for its cost-efficiency and allowing parents to react in a timely manner to their child’s request. It also offers the possibility to distinguish between the type or types of data collected and how the data will be shared publicly or with third parties. More stringent consent methods are only required when data is disclosed to third parties, thus allowing service operators to effectively obtain the necessary consent using methods reasonably geared to respond to the potential risk to privacy.

3. The age limit remains 13

In the 2012 revision, the FTC considered the option of extending the definition of a child to also include children aged 13 to 17. As a similar discussion is under way concerning the DPR proposal, it is important to consider the arguments brought forward in the COPPA debate. The key implementation issue with “scaling up” to the 13-17 age bracket is in dealing with anonymity. As noted in the New Yorker 20 years ago: “On the Internet, nobody knows you’re a dog.” Websites that have content directed to children are easy to define and rarely used by adults, so the

98 Federal Trade Commission, op.cit., Part 312, §312.2: “A website or online service shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link”.
99 Joshua Warmund, op.cit.
100 Id.
101 Berin Szoka and Adam Thierer, op.cit.
103 Berin Szoka and Adam Thierer, op.cit.
104 See Peter Steiner, 5 July 1993, On the Internet, Nobody Knows You’re a Dog, the New Yorker, available online at www.unc.edu/depts/jomc/academics/dri/idog.html, last accessed on 26 September 2013
enforcement of COPPA did not impact adults. However, expanding the legal definition of a “child” in COPPA would have meant that the parental consent requirement would impact websites that target adolescents and adults as well. As such, website operators would have to collect data from all users to allow children under 13 to access their websites. Moreover, it would prevent smaller operators from entering the market because of the stringent requirements, and thus, negatively affect competition.

4. COPPA provides incentives for self-regulation

The COPPA framework has built in incentives for industry self-regulation through the safe-harbour programmes. The four approved safe-harbours provide COPPA compliance by following the FTC proposed guidelines, and, in some cases, these commitments go further than the COPPA requirements. The advantages of self-regulation are two-fold. On the one hand, they ease burdens on regulatory arms to make sure the industry is compliant by outsourcing this to a third party. On the other hand, by joining a safe-harbour programme, website operators have the certainty that the restrictions applied by them are in line with COPPA requirements. Finally, safe-harbours may be quicker to react than the FTC in case of non-compliance and can also adapt to new technologies faster than statutory laws which must usually go through a lengthy regulatory process to be amended.

5. A flexible and workable legislative system

The Act tries to provide a flexible system which aims to allow industry to strike a balance between protecting the privacy of children and continuing to deliver goods and services that allow children to engage in creative, educational and playful activities. There is a clear distinction made between data collected for internal purposes only and data publically shared with third parties for marketing reasons. Data collection is required for maintaining or analysing the functioning of the website or online service, authenticating users, personalising content or protecting the security or integrity of the user, website or online service. Without proper evaluation of the services offered on the website or the popularity of the digital content, companies will have no incentive to offer child-oriented functionalities, so imposing parental consent requirements would actually result in less child-safe content. The framework recognises that the collection of personal data from a child for internal operations does not pose any privacy risks, exempting parental consent in this case.

In certain circumstances service operators should be allowed to collect and process limited information from children without having to request parental consent. The exemptions that COPPA provides come from years of experience and are crucial to the smooth operation of businesses. Operators may request the parent’s contact information and the child’s first name for the purpose of obtaining consent. Without this clear specification, the operator would have no legal way to actually contact the parent to obtain consent. Additionally, personal information may be collected without prior consent for “one-time use”. This exception allows children to interact with a website to retrieve a lost password or get homework help. In the absence of such a provision, this would burden parents with potentially unnecessary consent request for activities that do not actually pose a risk to the child, as well as complicate the user’s experience.
VI. Recommendations for the EU

As the European Union discusses and adopts new parental consent requirements for children, the Advertising Education forum gives the following recommendations:

- **Specific criteria should be determined to define what constitutes an “information society services directed to children”**. The definition should take into account several criteria, such as the type of visual content, the type of advertisements (if they are directed to children or not), the age of the characters featuring on the website, and the language used.

- **Provide incentives for industry representatives to develop best practice**. It is crucial not to cripple industry innovation and the development of newer and more efficient methods of obtaining parental consent. While it is important that certain methods of obtaining parental consent should be provided in a future framework, as initial guidelines, the DPR should also include built-in incentives for developing new, more efficient methods of obtaining consent. COPPA should be taken as a best-practice model in this case.

- **The so-called sliding scale method is the most cost effective and time-efficient method to obtain parental consent**. It allows for a proportionate system taking into account the privacy risks linked to the type of data collected and the intended purposes for collection.

- **Create enhanced protections for children under 13**. Imposing blanket restrictions to all minors under the age of 18 is not realistic and will not result in enhanced privacy protections for younger, more vulnerable children.

- **Consider all necessary exemptions for instances with limited/no privacy risk**. Any future parental consent mechanism will need to be proportionate and not excessively burdensome in order for parents and children alike to comply with it. The Regulation should therefore consider a series of scenarios that are exempted from the obligation to collect parental consent. Parental consent should only be necessary when a website operator has “actual knowledge” of dealing with children under the age of 13.
List of Sources

- **Legal documents**

  **European Commission** (25 January 2012) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on free movement of such data (General Data Protection Regulation), 2012/0011 (COD)


  **Korea** (2011) Enforcement Decree of the Personal Information Protection Act

  **The Parliament of the Commonwealth of Australia** (2012), Inquiry into Privacy Amendment (Enhancing Privacy Protection), A Bill for an Act to amend the law relating to privacy, and for other purposes

  **Québec** (1983) Consumer Protection Act of Quebec


- **Guidelines and Codes**

  **Federal Trade Commission** (2006) How to comply with the Children’s Online Privacy Protection Rule

  **Office of the Australian Federal Privacy Commissioner** (2001), Guidelines to the National Privacy Principles

  **UK Information Commissioner’s Office** (2010), Personal information online code of practice

- **Online publications and articles**

  **Tim Banks**, 18 October 2012, No “Do Overs”: Children, Personal Information and Marketing in Canada, *Data Governance Law*


  **Lynn Burke**, 29 February 2000, Time Running Out on Kid Email, *Wired.com*

  **Common Sense Media** (2011), Zero to Eight: Children’s Media Use in America, *Common Sense Media Research Study*

  **Leslie Haddon and Sonia Livingstone** (2012), EU Kids Online: national perspective, EU Kids Online, *the London School of Economics and Political Science*, London, UK


  **Jeff Jarvis**, October 2011, Do we Really Need to Protect Children From the Internet? *Time Ideas*

  **Osborne Clarke** (2012) The Data Gold Rush: Growing and protecting your position in the data ecosystem, Ipsos Mori


  **Denise Taylor**, 1 October 2006, It’s Time to Comply with COPPA, *iapp newsletter*

  **Adam Thierer**, 16 September 2011, Some Thoughts on FTC’s Proposed COPPA Revisions, *Tech Liberation*


- **Meeting transcript**