Response to the "Public Consultation on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule"

Completed by Eleonora Maria Mazzoli and Sonia Livingstone, Department of Media and Communications, London School of Economics and Political Science.

For further inquiries regarding this response, please contact: e.mazzoli@lse.ac.uk

Preferred citation: Mazzoli, E. M., and Livingstone. (2019) Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule. Evidence Review and Recommendations. London: London School of Economics and Political Science.

Key Recommendations

Children's autonomy and dignity depends on their freedom to engage and their freedom from undue persuasion or influence. In a digital age in which many everyday actions generate data – whether given by digital actors, observable from digital traces, or inferred by others, human or algorithmic – the relation between privacy and data online is complex. While recognising that COPPA is a U.S. Rule, its global impact on children is considerable, since they access many online services offered by U.S.-based companies that operate throughout the world, including in the United Kingdom (UK). We feel bound to advocate on behalf of those children and offer recommendations informed by evidence gathered from relevant academic literature, industry reports, and policy reflections in the UK and beyond.

With growing concerns over children's privacy and the commercial uses of their data, it is vital that children's understanding of the digital environment, their digital skills and their capacity to consent are considered in designing services, regulation and policy (Stoilova, Livingstone, and Nandagiri 2019, 3). Our position is grounded in the UN Convention on the Rights of the Child, and we define a child as all those aged under 18 years old.

Key messages:

a) **We ask the FTC to undertake an investigation to better understand children's data privacy and to examine business practices regarding digital content, advertising structures and data collection, including use of recently developed metrics** (such as "brand safety" targeting applications now in use by leading marketers and key platforms like YouTube and Facebook**).** The COPPA Rule and its implementation should reflect recent and ongoing developments in technologies.

b) **Any data collection and data processing linked to children, whether deliberate or otherwise, must be in the best interests of the child.** The child's best interests should be prioritised over commercial interests, and care should be taken in framing the regulation that compliance with the law does not undermine children's best interests or come at the cost of children's privacy and data protection.

c) **We urge clarification of the scope and definitions of the types of services covered by COPPA, and the definition of children's personal information.** We **support the inclusion of "inferred data"** (from profiling and other data analytics) in the definition of personal information.

d) We are particularly concerned that the **current definition of "directed to children" and "actual knowledge" do not adequately protect children**, since many services that are directed to adults are also directed to children or have a significant number of child users. Thus, services do have at least "constructed knowledge" that their users include children.

e) **We stongly support regulation for privacy-by-design and by-default** to require child-friendly age-appropriate mechanisms for privacy protection, complaint and remedy. Further work is needed to increase the transparency of data collection, improve privacy control navigation, enable granular control over privacy settings to match the elaborate data-harvesting techniques and create better industry standards for user empowerment.

f) We assert the importance of **a balanced approach between children's protection and their online participation**, for them to be safe and protected in today's digital era, while still benefiting from the great opportunities that it has to offer. To do so, we call on the FTC to investigate the impacts on teenagers of not being covered by the current COPPA Rule, and to propose safeguards also for those aged 13 to 17 years-old. This group could be hampered by overly stringent control mechanisms, and they particularly should be able to benefit from digital technologies and online services. All children's civil rights and freedoms, and their privacy rights are fundamental and the COPPA Rule and Act should ensure that young people aged 13-17 can fully exercise their rights and that they receive adequate data and privacy protection.

Urgent need for regulatory improvement

The COPPA Rule seeks to protect children on the internet through prohibitions on how online services - such as mobile apps, games and websites – collect, use, and disclose personally identifiable information (PII) from children, and how parents are informed and given control over those activities. However, not all operators are subject to COPPA, particularly those that "merely offer the public access to someone else's child-directed content" (78 Fed. Reg. 3977). While Google Play Store and Apple App Store have to implement some measures to help developers to comply with the law, numerous court cases and academic research have revealed problems in enforcement and compliance.[1]

All relevant stakeholders (app developers, distribution channels like platforms, third-party libraries such as app stores, and regulators) in this ecosystem should take actions to prevent the potential violations of children's privacy rights and more effectively protect children online. **There is an urgent need to ensure the effective implementation of the COPPA Rule, and to update the framework in response to an online environment where privacy is being reconfigured**.[2]

COPPA has become the de facto global standard for children's access to many internet sites and social media services around the world, and therefore its framework and actions matter globally. We urge the FTC to take into account such wider and perhaps unintended consequences of decisions that at first sight only seem to affect U.S. citizens.

[1] For instance, in 2018 a group of researchers has uncovered rampant potential violations of nearly 6,000 apps for children that points out current limitations of the COPPA Rule, especially of its enforcement (Reyes et al. 2018). Additional relevant articles available at: https://irwinreyes.com/assets/files/papers/2018-pets-coppa.pdf ; https://www.washingtonpost.com/news/the-switch/wp/2018/04/16/thousands-of-android-apps-may-be-illegally-tracking-children-study-finds/.

[2] Reference to Question (1) of FTC Consultation: *Is there a continuing need for the Rule as currently promulgated? Why or why not? Since the Rule was issued, have changes in technology/industry/economic conditions affected the need for or effectiveness of the Rule? What are the costs and benefits?*

Children's protection and participation online: a balancing act

In today's digital age, technologies are increasingly vital for children to exercise their rights and meet basic needs, as they provide much needed access to education, socialising, participation, wellbeing and entertainment. However, as technologies become more sophisticated, networked and commercially viable, children's privacy is threatened by new forms of data collection and surveillance enacted by businesses, parents, and the state, including schools, health and welfare systems and law enforcement (Stoilova, Livingstone, and Nandagiri 2019, 4). Children's specific needs and rights have been too little recognised or provided for by the digital environment and the regulatory, state and commercial organisations that underpin it (Livingstone et al, 2015). Achieving a holistic approach to children's "best interests" demands management of the **balance between protection and participation online** so that efforts to protect children do not have the consequence, intended or otherwise, of restricting children's opportunities.

Children (5-12 years-old) and teenagers (13-18 years-old) increasingly access content and information from a number of online sources (from OTT and video-sharing platforms to mobile apps and social media networks). Both children's capabilities and vulnerabilities should be considered when advancing more stringent rules for their navigation of the online digital environment. Many think critically about the websites they visit (Ofcom 2018, 11), and they in part grasp that a commercial data collection model underpins provision of the apps and services they use. However, they become critical and frustrated when their expectations of a fair internet are not met, when they feel they have little or no choice regarding the commercially exploitative practices of the services they want and need to use, and when nothing is done to respect their rights, explain the conditions of use in terms they can understand, or fix the problems they encounter and provide adequate remedy (Stoilova, Livingstone, and Nandagiri 2019, 37).

It is time to consider the full range of children's rights in a digital world, when revising regulation designed for their protection. Indeed, while children's issues are mainly considered in the context of child protection (from cyberbullying, abuse, and sexual exploitation), other child rights such as to privacy and freedom of expression are often overlooked. Nowadays, an unprecedented amount of information is being collected about people every day, to the extent that children have data footprints almost from the moment they are born. It is vital to consider privacy in its own right as well as a mediator of other rights in seeking a balance between child protection and participation online (Stoilova, Livingstone, and Nandagiri 2019).

It is evident from research that **children lack an adequate understanding of the processes of data collection and resultant commercial profiling and marketing to which they are subject** (ERGA 2018; ICO and Revealing Reality 2019). Simply providing more information to parents and children is insufficient for ensuring they can make informed decisions about their personal data (ICO and Revealing Reality 2019, 13). Instead, default limitations on the collection and use of personal data of children for both the development and application of user profiles for commercial purposes must be introduced (Verdoodt and Lievens, 2017; Montgomery and Chester, 2015). Whereas dominant business models are based on collecting as much data as possible, the best interests of children require restrictions on commercial profiling, taking into account the fact that for online services or advertising to be innovative and appealing to children, collecting and using children's personal data is not in itself a precondition. As highlighted by the preliminary ICO's and ERGA's reports on the UK's Age-Appropriate Design Code, differentiating between acceptable and unacceptable forms of sharing and using children's personal data requires a broad understanding of a wide variety of issues, ranging from the types of data involved to the purpose of the data usage or sharing (ERGA 2018; ICO and Revealing Reality 2019). Thus, in a commercial datafied world, stronger protections are vital.

Evidence of the risk of harm to children and related recommendations

We provide here some relevant evidence and research from European and UK studies, which is relevant for the questions outlined in the consultation and for the possible revision of the COPPA Rules. We have structured our response in two main sections. First, we will provide evidence and discuss the risk of harm for young children (under 13 years-old), secondly for teenagers (between 13 and 17 years-old). Emphasis is put on privacy-related risks of harm for associated with commercial practices, which are common for both age groups. Each section, we provide recommendations and responses to the questions outlined in the FTC consultation document (references to the relevant questions are included in the footnotes).

1. Risk of harm for young children (under 13 years old)

Supporting evidence

COPPA's definition of a child as "under 13" leaves millions of older children and teens with almost no specific data protection at all, during some of the most vulnerable years of their lives. The COPPA Rule FAQs already state that the FTC "is concerned about teen privacy and does believe that strong, more flexible, protections may be appropriate for this age group." New legislation, known as COPPA 2.0, has also been proposed by Senators Markey and Hawley, and would extend privacy protections to teenagers up to aged 16. In the UK and Europe regulators are increasingly acknowledging that all minors require additional protections for their data. For instance, although the EU's General Data Protection Regulation (GDPR) does not contain a definition of a 'child', the specific protection attributed to children when it comes to the processing of their personal data (recital 38) has been interpreted to apply to all children under the age of 18, in line with the United Nations Convention on the Rights of the Child (ICO, 2018; van der Hof and Lievens, 2018). In addition, the UK's Age Appropriate Design Code, set to become law in the next few months, is one example of a more principled-based approach to children's data protection. The Code extends its protections to all minors, not just under 13s, thus, challenging the status quo in which millions of young people aged 13-17 receive almost no specific data protection during some of the most vulnerable years of their life.

However, research shows that children of different ages have different understanding and needs. The truth of this claim does not mean it is easy to produce age groupings supported by evidence, nor that children fall neatly into groupings according to age; on the contrary, the academic community has largely moved beyond those early developmental psychology theories that proposed strict 'ages and stages'. Thus, while children develop their privacy-related awareness and literacy as they grow older, their development is multifaceted and complex; it does not fall neatly into simple stages and it varies based on their personal circumstances (Livingstone, Stoilova, and Nandagiri 2018). For example, a 15-year-old from a low socio-economic status (SES) home (DE) might have similar knowledge and digital literacy as an 11-year-old from a high SES home (AB) (Livingstone, Stoilova, and Nandagiri 2018).

Overall, a substantial body of literature discusses privacy online risks that children face: these are related, on the one hand, to the technological affordances and digital ecology, and on the other, to children's own online practices. As argued in a recent report by UNICEF, those fundamental dimensions of privacy affected by digital technologies include physical, communication, information and decisional privacy (UNICEF 2018, 8). Violations of physical privacy can take place in situations where the use of tracking, monitoring or live broadcasting technologies can reveal a child's image, activities or location. Threats to communication privacy instead relate to access to posts, chats and messages by unintended

recipients. Further, violations of information privacy can occur with the collection, storage and processing of children's personal data, especially if this occurs without their understanding or consent. Finally, disruptions of decisional privacy are associated with the restriction of access to useful information which can limit children's independent decision-making or development capacities.

In a recent report of the UK Information Commissioner Office (ICO) researchers Stoilova, Livingstone, and Nandagiri highlighted key issues and online risks for children that have come to the fore in their evidence review (Livingstone, Stoilova, and Nandagiri 2018). Among others, the most relevant risks derive from online marketing and commercial activities, awareness of and willingness to provide personal information online, the effects of privacy disclosures (including reputational damage, blackmailing, stalking or identify theft), issues related to participation on social networking sites, and unawareness of the online privacy policies of platforms (Livingstone, Stoilova, and Nandagiri 2018, 28-29). Within this context, s a 2018 study from the UK communication regulator Ofcom has reported that parents of children aged 5-15s who use the Internet are more likely to have concerns about seven areas: companies collecting information about what their child is doing online (50%); their child damaging their reputation (42%), the pressure on their child to spend money online (41%); giving out details to inappropriate people (41%); cyberbullying (40%); seeing content which encourages them to harm themselves (39%); and the possibility of the child being radicalised online (29%)(Ofcom 2018, 14).

The aforementioned concerns partially derive from the fact that means for processing children's data are advancing and multiplying rapidly, with commercial companies gathering more data on children than even governments do or can collect (UNICEF 2018), pushing commercial data collection to the top of the privacy concerns. Marketers employ many, often invasive, methods to turn children's activities into a commodity (Montgomery, Chester, and Milosevic 2017), monitoring of online use and profiling via cookie-placing, location-based advertising, contextual-based, filter-based, and behavioural targeting. Young consumers are often led to disclose personal information in exchange for enhanced online communication experiences (Bailey and Steeves 2017), or as a trade-off for participation and access to the digital services and products provided (Lapenta and Jørgensen 2015; Micheti, Burkell, and Steeves 2010).

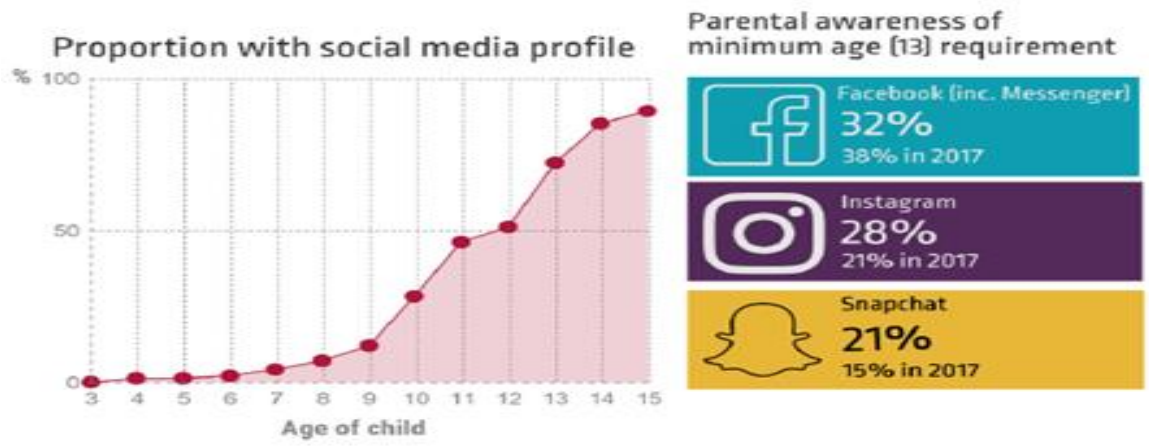
In particular, within the age group currently covered by the COPPA (under 13-year olds), existing studies suggest that children of this age are already starting to use online services which collect and share data. However, privacy awareness and digital media literacy widely differ among children. While on the one hand, some children may provide personal data passively and unconsciously when using online services like social media, provoked by the platform design and configuration (De Souza and Dick 2009; Madden et al. 2013; Pangrazio and Selwyn 2018). On the other hand, those who are tech-savvy still may feel obliged to agree with the Terms and Conditions and they see targeted advertising as a default part of contemporary life (Lapenta and Jørgensen 2015). As a result, they experience a contradiction between their desire to participate and the wish to protect their privacy, in a way that might cause a sense of powerlessness (Lapenta and Jørgensen 2015; Pangrazio and Selwyn 2018).

Furthermore, survey results and studies show that children are using services that are not officially covered by this regulatory framework, since they do not fall under their definitions as set forth in § 312.2 of the Rule. For example, in the UK, 52% of the children aged 3-4s go online for nearly 9h a week, 45% use YouTube, and 1% have a social media profile (Ofcom, 2018). Such numbers increase as the children grow older, moving from 82% of children aged 5-7s who go online for nearly 9 ½ h a week, to nearly 93% of kids aged 8-11s. Differences in the use of mainstream online services such as YouTube reduces with age as well, with 70% of kids aged 5-7s using YouTube compared to 77% of kids aged 8-11s (Ofcom, 2018). Instead, the use of social media seems to be more prominent at a later stage, as only 4% of kids aged 5-7s reported to have a social media profile, while there is a stark increase among teens with 18%

of children aged 8-11s and 69% of 12-15s are present on social media (Ofcom, 2018). Thus, children start developing a sense of ownership and independence already at this young age (Kumar et al. 2017), as they become confident internet users, but even if they engage in a narrow range of activities, they are still exposed to a number of risk while having a relatively low risk awareness (Bakó 2016; McReynolds et al. 2017).

Children's sharing of personal data at a young age is primarily guided by parental advice (Livingstone 2008), and those whose parents are actively mediating their internet use are sharing less personal information online (Miyazaki, Stanaland, and Lwin 2009). Nevertheless, parental control is not sufficient, as parental awareness and tech-savviness also widely differs among parents depending on a number of variables, such as educational level, cultural background, societal status. For instance, as a recent Ofcom's report shows (see Figure 1), only 32% of UK parents are aware of the minimum age requirements for Facebook, 28% of Instagram and 21% of Snapchat (Ofcom 2018, p. 17). Thus, reinforcing parent control mechanisms, such as parental consent, or extending such mechanism to all minors (i.e. under 18-years old), might cause more unintended consequences than positive impacts for children (see following section).

Figure 1. Social media use by age and awareness of minimum age requirements, among parents whose child has relevant social media. Source: Children and Parents: Media Use and Attitudes Report 2018 (Ofcom 2018).



In addition to the privacy-related risks, going online can expose children to unwanted experiences. As Ofcom's survey highlights, in 2017, around one in ten 8-11s and one in five 12-15s said they had ever personally experienced some form of bullying; one in eight 12-15s said they had been bullied either face to face (12%), or on social media (11%); and 9% said they had been bullied through messaging apps or by text (Ofcom 2018, p. 12). Alongside cyberbullying and online harassment, the study found that 16% of children aged 8-11 who go online have ever seen something online that they found worrying or nasty, but at 31%, 12-15s are nearly twice as likely to have experienced this (Ofcom 2018, p. 12). In particular, the types of concerns among UK adults of potential children's harm relating to content ranges from unsuitable content for children and online misinformation, to child exploitation, promotion of terrorism/radicalisation, pornography and violence (ICO and Ofcom 2018, 7)[3].

[3] Ofcom and ICO (2018). Internet users' experience of harm online 2018. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0018/120852/Internet-harm-research-2018-report.pdf

As highlighted by the UK Government in its Online Harms White Paper (Department for Digital Culture Media and Sport and Home Office 2019, 12-22), these concerns stem by existing threats presented for instance by online CSEA (child sex exploitation and abuse),[4] violent and hatred content shared online,[5] and abusive and offensive communications online, which often characterise certain online services.[6] The 2018 Doteveryone Digital Attitudes Report found that users perceive the presence of anonymous abusive and offensive communications almost as an unavoidable characteristic of online service, as they perceive that the market currently offers very few safer alternatives of online services, thus, they feel that they have no choice but to sign up, even if they had concerns or bad past experiences on such platforms (Doteveryone 2018).[7] Within this scenario, the UK Government stated that existing efforts by private and public organisations aimed to tackle harmful content have not yet delivered the necessary improvements, thus, "creating an urgent need for government to intervene to drive online services to step up their response" (Department for Digital Culture Media and Sport and Home Office 2019, 12).

Existing legal and regulatory frameworks like the COPPA Rule and Act have laid the ground for increased children's protection online; however, given the fast-pace of technological innovation, there is clearly a need to update this set of rules. Even though these policies proved to have positive impacts on children's protection by improving online services and pushing towards the adoption of industry codes of conduct and best practices, further implementation and enforcement work is needed. In fact, even though the Rule has affected significantly data collection practices, a number of court cases and research studies have shown rampant potential violations of this regulation that points out its current limitations, especially of its enforcement.[8] For instance, in a recent publication, a group of U.S. researchers analysed nearly 6,000 apps for children and found that the majority of them may be in violation of the COPPA, since the study found that thousands of the tested apps collected the personal data of children younger than 13 without a parent's permission law (Reyers et. al 2018).[9]

Moreover, the FTC has moved against a number of app developers and third-party service providers for gathering PII from children, finding a number of companies because they violated the COPPA Rule. Until now, fines for failing to comply with the law are up to $41,484 per privacy violation per child (for a

[4] The internet Watch Foundation (IWF) estimates that 55% of the child sexual abuse material they find online contains children aged ten or under, and 33% of this imagery is in the most serious category of abuse (IWF, 2017, available at: https://annualreport.iwf.org.uk/). In 2018 there were over 18.4 million referrals of child sexual abuse material by US tech companies to the National Center for Missing and Exploited Children (NCMEC). Of those, there were 113, 948 UK-related referrals in 2018, up from 82,109 in 2017 (NCMEC, Available at: http://www.missingkids.com/footer/media/vnr/vnr2)

[5] The Internet Watch Foundation report shows that youth rival gangs use social media to glamorise weapons and gang life, as well as to directly depict or incite acts of violence. Alongside the illegal sale of weapons to young people online, this is a contributing factor to incidents of serious violence, including knife crime, in the UK. The latest police recorded crime figures, for the year ending September 2018, show an 8% increase in knife crime (to 39,818 offences) compared with the previous year. Homicide figures have risen by 14% (excluding terrorist attacks) over the same period (Internet Watch Foundation 2017, Available at: https://annualreport.iwf.org.uk/)

[6] The Law Commission noted that in many cases of harassment and other forms of abusive communications online, the offender will be unknown to the victim. In some instances, they will have taken technical steps to conceal their identity. Government and law enforcement are taking action to tackle this threat.

[7] Doteveryone 2018 report available at: https://attitudes.doteveryone.org.uk/files/People%20Power%20and%20Technology%20Doteveryone%20Digital%20Attitudes%20Report%202018.pdf

[8] Reference to Questions 2, and 3 of FTC Consultation: (2) *What effect, if any, has the Rule had on children, parents, or other consumers? Has the rule benefited/imposed costs on children, parents, or other consumers? (3) What impact, if any, has the Rule had on operators? Has the rule benefited/imposed costs on operators?*

[9] Research study available at: https://irwinreyes.com/assets/files/papers/2018-pets-coppa.pdf ; https://www.washingtonpost.com/news/the-switch/wp/2018/04/16/thousands-of-android-apps-may-be-illegally-tracking-children-study-finds/

comprehensive list of the most relevant violation, visit PRIVO's website).[10] While on the one hand, these cases show that the FTC is monitoring the correct implementation of the COPPA Rule; on the other hand, they also demonstrate that its industry-led enforcement is still failing. Moreover, even those aforementioned FTC decisions raise a number of questions that still need to be answered. In the Google case for instance, the FTC asked Google to no longer target children with data-driven marketing and advertising on YouTube programming targeted to kids. Even though Google announced that they will do so as of January 2020, how will these new policies actually be implemented and monitored? How will it treat programming classified as "family viewing"—exempt it from the new data targeting safeguards? How will YouTube influencers' channels and content targeting children be covered by these policies? (Chester, 2019). These are just some of the questions that should be addressed both by the FTC to ensure forward-looking safeguards for children, as well as, by companies and service providers like Google. Furthermore, in alignment with the statement of the Centre for Digital Democracy (CDD), we also believe that the company should prohibit such data targeting practices on all minors on YouTube worldwide, but it is necessary that both the FTC and Google provide further clarify on how this will be achieved (Chester, 2019).[11]

Recommendations

Given the previously discussed risks and threats to children and the ongoing developments of the digital environment they live in, there is clear evidence that some of the definitions set forth in § 312.2 of the Rule are inadequate and do not accomplish COPPA's goal of protecting children's online privacy and safety.[12] In particular, covering under the scope of the Rule only services "directed to children" or that

[10] For instance, after increasing pressures and complaints from a number of organisations and institutions, such as the CCFC, CDD and IPR in 2015 concerning Google's child-directed practices (on YouTube, YouTube Kids app and elsewhere), finally the FTC took a historic and highly decision which resulted in one of its biggest case: Google Alphabet has been fined $170 million for violation of children's privacy on YouTube as the site has been accused of collecting data on children's under 13 without parental consent, and used for monetization strategies and targeted advertising. FTC's decision on Google's YouTube service resulted also from the filed complaints and documentation provider by the Campaign for Commercial-Free Childhood (CCFC), our attorneys at the Institute for Public Representation (IPR) at Georgetown University Law Center, and a broad coalition of consumer, privacy, public health and child rights groups. Further information on the documentation provided can be found here: https://www.prnewswire.com/news-releases/smarty-pants-report-finds-youtube-is-kids-most-loved-brand-300502382.html. The news was communicated by the FTC, and it is still being discussed both in the U.S. (e.g. https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.htm); as well as in other countries like the UK (https://www.bbc.co.uk/news/technology-49578971), given the repercussions that such decision could have on a service that is being globally used by children around the world. The second biggest and most recent case instead regards Tik Tok (previously known as video social networking app Musical.ly), which has been fined $5.7 million because it failed to provide direct notice of its information practices to parent, to obtain verifiable parent consent prior to collection, use and disclosure of children's personal information and to delete personal information at the request of parents. The news was communicated by the FTC (press release available at: https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc), and it made the headlines of a number of news sources.

[11] Article by CDD-Centre for Digital Democracy, 2019, available at: https://www.democraticmedia.org/article/ftcs-googleyoutube-decision-childrens-privacy-digital-marketing-brings-new-safeguards

[12] Reference to Questions 9, 10, 14, and 15: (*9) Do the definitions set forth in § 312.2 of the Rule accomplish COPPA's goal of protecting children's online privacy and safety? (10) Are the definitions in § 312.2 clear and appropriate? If not, how can they be improved, consistent with the Act's requirements? (14) Should the definition of "Support for the internal operations of the website or online service" be modified? Are there practices in addition to behavioural targeting and profiling that should be expressly excluded from the definition?* Should additional *activities be expressly permitted under the definition? (15) Does § 312.2 correctly articulate the factors to consider in determining whether a website or online service is directed to children? Do any of the current factors need to be clarified? Are there additional factors that should be considered? For example, should the definition be amended, consistent with the statute, to better address websites and online services that do not include traditionally child-oriented activities, but that have large numbers of child users?*

have "actual knowledge"[13] that children are on their services is highly limiting and does not provide adequate protection. Crucially, "services directed to children" does not include mixed audience services that do not target children as their primary audience, provided they deny access to anyone who self-reports as under 13-years old, such as Facebook and YouTube. Thus, in practice, this definition has allowed services to avoid being subject to COPPA simply by asking users to self-report their age and then only admitting users who say they are over 13-years old.

However, there is plenty of evidence that also children under 13-years old are using such platforms, and therefore, **we would urge the FTC to re-examine its interpretation of "child-directed content and services". To achieve so, the FTC could enforce its interpretation of both this definition as well as the definition of "actual knowledge" (present in the COPPA Act) in a more stringent way, including also what can be described as "constructed knowledge" i.e. what an operator ought to know about its users if they have carried their work in due diligence.**[14] However, we would like to emphasise that there should be a limitation to what data is justifiably collected in order to reach such "actual" or "constructed knowledge".

We argue that in commercial and institutional practices there are different types of children's data that should be protected from exploitation, monetization and profiling, including "inferred data". By "inferred data" we refer to the data derived from analysing data given and data traces, often by algorithms (also referred to as 'profiling'), possibly combined with other data sources (Livingstone, Stoilova, and Nandagiri 2018, 16). Therefore, we would support the inclusion of "inferred data" in the COPPA's definition of "personal information", which is "information that relates to an identified or identifiable individual", as defined by the UK Information Commissioner's Office (ICO) and the EU General Data Protection Regulation (GDPR). A practical example of such inclusion can be found in the implementation of Right to data portability in the UK, where ICO stated that "*inferred* or *derived* data is personal data" and should therefore be protected under the current data protection and privacy frameworks.[15]

Moreover, **we call for introducing privacy-by-design and by-default. Such regulation should entail default limitations to the collection and use of children's personal data for commercial purposes.** For instance, in relation to online profiling data processing processes can be designed in ways that automatically rule out personal data which holds attributes pertaining to persons under eighteen as well as refrain from applying the results of profiling processes to children (Lievens et al, 2019). A child-centred approach to privacy-by-design and by-default allows for the protection of children's personal data to be built into data processing systems, without children and parents having to fully comprehend the complexity of these systems. Moreover, such regulation should also provide child-friendly age-appropriate mechanisms for privacy protection, complaint and remedy, as ease of use, ubiquitous functions and user-friendly features of privacy setting interfaces may reinforce children's privacy protection behaviours (Stoilova, Livingstone, and Nandagiri 2018).

Finally, we want to highlight that children cannot be expected to be solely responsible for handling the complex privacy environment, nor the responsibility for their protection should be on parents (Stoilova,

[13] Actual knowledge is generally understood to be 'the direct and clear awareness of a fact or circumstance', while constructive knowledge is understood as knowledge that a person should have if they had made the usual and proper inquiries.

[14] Constructed knowledge is generally defined as knowledge and information constructed and found when researching, questioning and analysing what is legally available.

[15] For more on 'personal data' see "What is personal data?" available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-ppersonal-data/; and "The right to data portability" available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

Livingstone, and Nandagiri 2018). **Responsibility should be shared with all relevant stakeholders involved, including those commercial companies providing platforms services that are used by children.** Thus, **these private actors should also be required to conduct privacy impact assessments, whenever they want to develop online services that (might) entail the processing of personal data of children.** When undertaking such an impact assessment, companies should consider children's rights to protection as well as to participation and take the best interests of the child as a primary consideration (Verdoodt and Lievens 2017; Lievens and van der Hof 2018). Further work is therefore urgently needed to **increase the transparency of data collection, improve privacy control navigation, enable granular control over privacy settings to match the elaborate data-harvesting techniques and create better industry standards around user empowerment.**

2. Risk of harm for teenagers (13 to 17 years-old)

Supporting evidence

Firstly, we wanted to highlight that those privacy-related risks discussed in the previous section are as important for young children under 13 years as for all minors (under 18 years-old). [16]Online platforms and digital technologies provide opportunities for development (while also introducing and amplifying risks) that children can use to build the skill entourage that they need for their growth (Livingstone 2008). There is also solid evidence that understanding of privacy becomes more complex with age and that the desire for privacy also increases (Chaudron, Gioia, and Gemo 2018; Kumar et al. 2017). Thus, while we believe that while both under 13s and teens aged 13-17 should be adequately protected online, we urge the FTC to also take into account some unintended consequences and mistaken assumptions of raising the age of all provisions included in the COPPA Rule and Act, especially, introducing overly stringent control mechanism for teens.

Foremost, we strongly believe that online safety, data protection and privacy provisions included in the COPPA Rule should be extended to all minors, thus, including teenagers from 13-17. It is increasingly accepted that using the internet carries some risk of harm for all minors, and even though risks do not inevitable result in harm, but rather concern factors that raise the probability of harm (Livingstone, 2013), it is pivotal to address them in regard to all vulnerable groups, including teenagers.[17] While on the one hand, not all these concerns and risks can be related to violations of the COPPA Rule, on the other hand, we know that children's privacy and data protection violations, as well children's encounters with upsetting content happen on services that are relevant for the implementation of the COPPA Rule, like video-sharing sites (e.g. YouTube), social networking sites (SNSs), games, or instant messaging apps (Livingstone et al., 2014). In addition, personal data exploitation (e.g. monetisation, commercial exploitation, profiling, targeted advertising etc.) and misuses (e.g. privacy breaches, release of personal information to third parties for sharing, selling, rending or transfer of personal information

[16] Privacy is indeed vital for all children's development, and as research shows, key privacy-related media literacy skills are closely associated with a range of child developmental areas – autonomy, identity, intimacy, responsibility, trust, pro-social behaviour, resilience, critical thinking and sexual exploration (Balleys and Coll 2017; Pradeep and Sriram 2016; Raynes-Goldie and Allen 2018; Valkenburg and Jochen 2011).

[17] Numerous studies and research have widely demonstrated that there are many online risks encountered by teenagers, including aggression and violence of various kinds (e.g. bullying, aggression, and hate); sexual harms to children (e.g. sexual harassment, sexting); problems associated with inappropriate or damaging values; and data collection activities associated commercial/persuasive/manipulative risks for all minors (UKCCIS, 2018, 25-26). For additional data and information see UKCCIS Evidence Group 2017 report available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759005/Literature_Review_Final_October_2017.pdf

etc.) have serious impacts for all minors. Therefore, the current scope of the COPPA Rule to children under 13 years-old is extremely limiting and it does not achieve the overarching aim of the regulation.[18]

Whereas we strongly support the extension of relevant provisions under the COPPA Rule and Act to 13-17 year-old children, to protect their privacy, we do not support raising the age for parental consent or controls. On the contrary, such measure does not address some underlying mistaken assumptions and it may bring unintended consequences for the development of children.[19] If parents manage access, and monitor use of teens' online activities, a number of additional problems may arise depending on the relationships that teens have with their parents, their family context and personal situation. Some of the main issues that could result include (a) a chilling effect on teens' freedom of expression; (b) a violation of privacy for teens' who need health/sexual/political information that their parents may act to prevent if aware; (c) a violation of the safety of teens who need to access online help and support services to report problems within the home; (e) an increase in teens' use of hidden, encrypted, secret or deceptive services (including the dark net, VPNs etc.) that make it harder to provide them with outside help when needed, (f) and an overall breakdown of trust between child and parent. Thus, increasing parental oversight and control does not imply increased protection for teens, and a more nuanced and balanced approach is needed to achieve a regulatory framework that is adequate for teens' online experiences.

Furthermore, assuming that consent and children's media regulation should sit with the parents is not only burdensome but, in some cases, also inequitable and counter-productive. The fact that the digital ecosystem has evolved so rapidly means that parents are not always able to keep up. Thus, more educated and tech-savvy parents would be the only ones capable of effectively guiding their children's media choices and habits. Further, by giving parents the authority and control over children's media uses also absolves corporate companies and public institutions, like educational system, cultural and media institutions, of the responsibility to make the internet a good place for children. Furthermore, age segregation does not necessarily lead to stronger children's protection. On the contrary, the right kinds of mixed age and intergenerational supports can keep children safe and help them to become good and savvy digital citizens. Thus, judgements concerning access to content, information and services online, as well as access and use of personal data are complex and require a shared responsibility of families, corporate companies and institutions.

Recommendations

Given the evidence hereby provided, we strongly believe that is necessary to reach a balanced approach between minors' protections and their online participation, in order for them to be safe and protected in today's digital era, while still benefiting from the great opportunities that it has to offer. To do so, **we call the FTC to investigate the adverse impacts on teenagers of not being covered by the current COPPA Rule, and to propose safeguards also for 13 to 17 years-old.** This group could be hampered by overly stringent control mechanisms and we do believe that teens should be able to go online and benefit from digital technologies and online services without parental control. However, teens' privacy rights are fundamental and the COPPA Rule should ensure that also young people aged 13-17 receive adequate data and privacy protection, in particular against commercial practices, such as profiling,

[18] Reference to Question 9: (*9) Do the definitions set forth in § 312.2 of the Rule accomplish COPPA's goal of protecting children's online privacy and safety?*

[19] Reference to Questions 19 and 21: (19) *Has the consent requirement been effective in protecting children's online privacy and safety? What data exist on: (1) Operators' use of parental consent mechanisms; (2) parents' awareness of the Rule's parental consent requirements; or (3) parents' response to operators' parental consent requests?* (21) *COPPA and § 312.5(c) of the Rule set forth eight exceptions to the prior parental consent requirement. Are the exceptions in § 312.5(c) clear and appropriate?*

monetisation, targeted content and advertising strategies etc. These practices raise indeed a number of concerns and risks of harm for all minors, thus, we believe that stronger protections are needed for both children under 13 years-old and teens under 18 years-old.

References

Acker, Amelia, and Leanne Bowler. 2018. 'Youth Data Literacy: Teen Perspectives on Data Created with Social Media and Mobile Devices'. In Hawaii, 10.

Bailey, Jane, and Valerie Steeves. 2017. 'Introduction: Cyber-Utopia? Getting Beyond the Binary Notion of Technology as Good or Bad for Girls'. In *EGirls, ECitizens*, Droit, technologie et médias | Law, Technology and Media, Ottawa: Les Presses de l'Université d'Ottawa | University of Ottawa Press, 1–17. http://books.openedition.org/uop/487 (October 17, 2019).

Bakó, Rozália Klára. 2016. 'Digital Transition: Children in a Multimodal World'. : 11.

Balleys, Claire, and Sami Coll. 2017. 'Being Publicly Intimate: Teenagers Managing Online Privacy'. *Media, Culture & Society* 39(6): 885–901.

Bowler, Leanne, Amelia Acker, Wei Jeng, and Yu Chi. 2017. '"It Lives All around Us": Aspects of Data Literacy in Teen's Lives'. In Washington, DC, USA, 27–35. https://www.researchgate.net/publication/320587868_It_lives_all_around_us_Aspects_of_data_literacy_in_teen's_lives (October 18, 2019).

Chaudron, Stephane, Rosanna Di Gioia, and Monica Gemo. 2018. *JRC Science for Policy Report. Young Children (0-8) and Digital Technology: A Qualitative Study across Europe*. European Commission.

Chester, Jeff. 2019. *The FTC's Google/YouTube decision on children's privacy & digital marketing brings new safeguards, opportunities—and questions.* CDD Newsroom. https://www.democraticmedia.org/article/ftcs-googleyoutube-decision-childrens-privacy-digital-marketing-brings-new-safeguards

Children's Commissioner for England. 2017. *Growing Up Digital. Taskforce Report*. London: Children's Commissioner England. https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf (October 17, 2019).

De Souza, Zaineb, and Geoffrey N. Dick. 2009. 'Disclosure of Information by Children in Social Networking—Not Just a Case of "You Show Me Yours and I'll Show You Mine"'. *International Journal of Information Management* 29(4): 255–61.

Department for Digital Culture Media and Sport, and Home Office. 2019. *Online Harms White Paper*. www.gov.uk/government/publications.

Doteveryone. 2018. *People Power and Technology: The 2018 Digital Attitudes Report*. Doteveryone. https://attitudes.doteveryone.org.uk/files/People%20Power%20and%20Technology%20Doteveryone%20Digital%20Attitudes%20Report%202018.pdf.

Emanuel, Lia, and Danaë Stanton Fraser. 2014. 'Exploring Physical and Digital Identity with a Teenage Cohort'. In *Proceedings of the 2014 Conference on Interaction Design and Children - IDC '14*, Aarhus, Denmark: ACM Press, 67–76. http://dl.acm.org/citation.cfm?doid=2593968.2593984 (October 18, 2019).

ERGA. 2018. *ERGA Academy 2018 Workshop: Protecting Children in Audiovisual Media Services - the Effectiveness of Age Verification and Media Literacy*. Activity report.

EU Kids Online. http://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online

ICO. 2018. Children and the GDPR. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/ (20 November, 2019).

ICO, and Ofcom. 2018. *Internet Users' Experience of Harm Online: Summary of Survey Research*. Information Commissioner's Office and Ofcom. https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/internet-use-and-attitudes/internet-users-experience-of-harm-online.

ICO, and Revealing Reality. 2019. *Towards a Better Digital Future. Informing the Age Appropriate Design Code*. Information Commissioner's Office.

Internet Watch Foundation. 2017. 'Internet Watch Foundation: Annual Report 2017'. https://annualreport.iwf.org.uk/ (October 17, 2019).

Kumar, Priya et al. 2017. '"No Telling Passcodes out Because They're Private": Understanding Children's Mental Models of Privacy and Security Online'. *Proc. ACM Hum.-Comput. Interact.* 1(CSCW): 64:1–64:21.

Lapenta, Gry Hasselbalch, and Rikke Frank Jørgensen. 2015. 'Youth, Privacy and Online Media: Framing the Right to Privacy in Public Policy-Making'. *First Monday* 20(3). https://firstmonday.org/ojs/index.php/fm/article/view/5568 (October 17, 2019).

Lievens, E. et al. 2019. The child right to protection against economic exploitation in the digital world. Submission to the Committee on the Rights of the Child in view of their intention to draft a General Comment on children's rights in relation to the digital environment (May 2019). https://www.ohchr.org/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/OtherStakeholders/EvaLievensSimonevanderHofetal.pdf (November 20, 2019).

Livingstone, Sonia. 2008. 'Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression'. *New Media & Society* 10(3): 393–411.

———. 2013. *Children and the Internet*. John Wiley & Sons.

———. 2013. "Online risk, harm and vulnerability: Reflections on the evidence base for child internet safety policy." *ZER: Journal of Communication Studies* 18(35), 13-28. Retrieved from http://eprints.lse.ac.uk/62278/.

Livingstone, Sonia, Haddon, Leslie., Görzig, Anke, and Ólafsson, Kjartan. 2010. *Risks and safety on the internet: The UK report*. London: EU Kids Online, London School of Economics and Political Science. Retrieved from http://eprints.lse.ac.uk/33730/.

———. 2011. *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries*. EU Kids Online, Deliverable D4. EU Kids Online Network, London, UK.

Livingstone, Sonia, Mariya Stoilova, and Rishita Nandagiri. 2018. *Children's Data and Privacy Online: Growing up in a Digital Age. An Evidence Review*. London: London School of Economics and Political Science. http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf.

Livingstone, Sonia, and Smith, P. K. 2014. "Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age." *Journal of Child Psychology and Psychiatry* 55(6), 635-54. doi:10.1111/jcpp.12197

Lupton, Deborah, and Ben Williamson. 2017. 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights'. *New Media & Society* 19(5): 780–94.

Madden, Mary et al. 2013. *Teens, Social Media, and Privacy*. Pew Research Centre. https://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/ (October 18, 2019).

McReynolds, Emily et al. 2017. 'Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys'. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*, Denver, Colorado, USA: ACM Press, 5197–5207. http://dl.acm.org/citation.cfm?doid=3025453.3025735 (October 17, 2019).

Micheti, Anca, Jacquelyn Burkell, and Valerie Steeves. 2010. 'Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand'. *Bulletin of Science, Technology & Society* 30(2): 130–43.

Miyazaki, Anthony D., Andrea J. S. Stanaland, and May O. Lwin. 2009. 'Self-Regulatory Safeguards and the Online Privacy of Preteen Children: Implications for the Advertising Industry'. *Journal of Advertising* 38(4): 79–91.

Montgomery, Kathryn C., Jeff Chester, and Tijana Milosevic. 2017. 'Children's Privacy in the Big Data Era: Research Opportunities'. *Pediatrics* 140(Supplement 2): S117–21.

Murumaa-Mengel, Maria. 2015. 'Drawing the Threat: A Study on Perceptions of the Online Pervert among Estonian High School Students'. *YOUNG* 23(1): 1–18.

Nairn, Agnes. 2012. 'Consumer Kids - the Influence of the Commercial World on Our Children'. *Education review* 22(1): 54–60.

Ofcom. 2018. *Children and Parents: Media Use and Attitudes Report 2018*.

Pangrazio, Luci, and Neil Selwyn. 2018. '"It's Not Like It's Life or Death or Whatever": Young People's Understandings of Social Media Data'. *Social Media + Society* 4(3): 2056305118787808.

Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, Massachusetts: Harvard University Press.

Pradeep, Pooja, and Sujata Sriram. 2016. 'The Virtual World of Social Networking Sites: Adolescents' Use and Experiences'. *Psychology and Developing Societies* 28(1): 139–59.

Raynes-Goldie, Kate, and Matthew E. Allen. 2018. 'Gaming Privacy : A Canadian Case Study of a Co-Created Privacy Literacy Game for Children'. *Surveillance and society* 12(3): 414–26.

Reyes, Irwin et al. 2018. '"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale'. *Proceedings on Privacy Enhancing Technologies* 2018(3): 63–83.

Stoilova, Mariya, Sonia Livingstone, and Rishita Nandagiri. 2019. *Children's Data and Privacy Online: Growing up in a Digital Age. Research Findings*. London: London School of Economics and Political Science. http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline.

UKCCIS. 2017. *Children's online activities, risks and safety: A literature review by the UKCCIS Evidence Group.* UKCCIS-UK Council for Child Internet Safety. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759005/Literature_Review_Final_October_2017.pdf

UNICEF. 2018. *Industry Toolkit. Children's Online Privacy and Freedom of Expression*. UNICEF. https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf.

Valkenburg, Patti M., and Peter Jochen. 2011. 'Adolescents' Online Privacy: Toward a Developmental Perspective'. In *Privacy Online: Theoretical Approaches and Research Perspectives on the Role of Privacy in the Social Web*, S. Trepte & L. Reinecke. https://www.researchgate.net/publication/279190144_Adolescents'_Online_Privacy_Toward_a_Developmental_Perspective (October 17, 2019).

van der Hof, S. and Lievens, E. 2018. "The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR", *Communications Law* 2018, Vol. 23, No. 1.

Verdoodt, V. and Lievens, E. 2017. Targeting children with personalised advertising – How to reconcile the (best) interests of children and advertisers. In *Data Protection and Privacy under Pressure*, Vermeulen G. andLievens E., Antwerp: Maklu, 313-341.

Zuboff, Shoshana. 2015. 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization'. *Journal of Information Technology* 30(1): 75–89.

———. 2019. 'Surveillance Capitalism and the Challenge of Collective Action'. *New Labor Forum* 28(1): 10–29.