Privacy Vaults Online, Inc., d/b/a PRIVO
17949 Main St., #1025
Dumfries, VA 22026-1025
PRIVO.com

December 11, 2019

VIA ELECTRONIC SUBMISSION

April J. Tabor
Acting Secretary
Federal Trade Commission
600 Pennsylvania Avenue, NW
Suite CC-5610 (Annex B)
Washington, DC 20580

Re: Comments of PRIVO
Rule Review, 16 CFR part 312, Project No. P195404

Dear Ms. Tabor:

Privacy Vaults Online, Inc. d/b/a/ PRIVO, an authorized Safe Harbor provider under the Children's Online Privacy Protection Act ("COPPA") submits its Comments in response to the Federal Trade Commission's Request for Public Comment[1] in its review of its rules and regulations implementing the Children's Online Privacy Protection Act (the "COPPA Rule").[2]

PRIVO has served as an FTC-approved COPPA Safe Harbor for more than 15 years, and has participated extensively in all Commission proceedings addressing COPPA and in Safe Harbor roundtables, lending its extensive experience to help inform the Commission and industry on issues of children's privacy and developments in the marketplace affecting it. PRIVO strives to fulfill the Commission's expectation that Safe Harbors move quickly to address new practices and changes in the marketplace as well as to innovate and, where possible approve, new solutions for verifiable parental consent. PRIVO was the first to use government issued data via a combination of last name, date of birth and the last for digits of social security number in securing meaningful parental consent to child participation online, which the FTC later codified as an enumerated method in the COPPA Rule. PRIVO has the first to market GDPRkids™ Privacy Assured Program and a secure privacy enhanced and interoperable family friendly identity and consent management platform compliant with both regulations. PRIVO also, via its work with the National Institute of Standards and Technology (NIST), co-authored the Minor's Trust Framework available on the OIX Registry which facilitates ecosystem-wide compliance solutions for those participants adopting its principles for protection of child privacy online. Most recently, PRIVO was pleased to participate as a panelist in the Commission's October 2019 COPPA Workshop.[3]

When Congress adopted the Children's Online Privacy Protection Act in 1998, it was forward thinking and proactive legislation designed to help safeguard children under 13 in the rapidly evolving online

[1] https://www.federalregister.gov/documents/2019/07/25/2019-15754/request-for-public-comment-on-the-federal-trade-commissions-implementation-of-the-childrens-online

[2] 16 CFR. Part 312.

[3] See https://www.ftc.gov/news-events/events-calendar/future-coppa-rule-ftc-workshop.

ecosystem. Yet, it sought to do so by striking a balance between permitting children to engage with and benefit from the Internet and connected technologies on the one hand, and empowering parents to protect their children's personal information online, on the other. Today, some 20 years on, the Act and the Commission's COPPA Rule implementing it remain as relevant and even more necessary than when they were first adopted. The sliding scale of parental consent currently embodied in the COPPA Rule is a key element that offers several low burden means of compliance to permit appropriate child engagement in those environments where the risk to child privacy is also low, while requiring higher safeguards and levels of assurance where risk is higher, such as via sharing, public disclosure or profiling. Both PRIVO and the Centre for Information Policy Leadership have recommended this model of privacy protection to regulators developing guidance for the implementation of the General Data Protection Regulation (GDPR) in relation to children.[4]

But, more can be done to the fulfill the promise of this groundbreaking and important legislation. Of great importance is the need for more research, workshops, working groups and consumer and stakeholder education about the advertising marketplace and the marketplace surrounding educational institutions. This continuing updating is needed not only to better regulate the system and protect privacy but to dispel significant misperceptions among stakeholders that COPPA only addresses whether content shown to children is appropriate, and that COPPA causes insurmountable conflicts with other regulations and business models. Where COPPA is perceived to be no more than the online equivalent of movie ratings designed to prevent children from seeing scary content or hearing swear words, its requirements are not taken seriously with the result that many call for its protections to be weakened. In PRIVO's experience, however, industry and users both benefit when COPPA-compliant child privacy safeguards are in place permitting children, content creators, and brands to interact in appropriate ways.

I. General Questions for Comment

A. Continuing Need For and Costs/Benefits of the COPPA Rule

In its Questions 1 through 3 of the Request for Public Comment, the Commission seeks information about the continuing need for the COPPA Rule (and the 2013 amendments to it in particular) as well as the Rules's costs and benefits for children, parents, and operators. At Question 4, the Commission asks specifically about the costs and benefits of the COPPA Rule as it relates to small businesses. In response to these questions, PRIVO can emphatically affirm that the protections embodied in COPPA and the Commission's COPPA Rule are still needed and that the changes in the online marketplace that have occurred since their adoption only reinforce that continued vigilance and innovation, as well as regulator, consumer and content creator education, are needed to keep pace with the rapidly changing online ecosystem.

In PRIVO's experience, both children and operators benefit when COPPA-compliant processes are in place to permit operators to offer relevant content to children and permit children to engage with that content in an appropriate and permissioned manner. Operators can serve contextual advertising, which helps pay for the creation of the content, to an audience that it knows contains children or children and

[4] The GDPR is applicable to any entity processing the personal data of data subjects in the European Union and European Economic area or any entity established as a controller in the EU processing personal data of data subjects globally. Similarly, COPPA is applicable to US companies' data collection from children regardless of jurisdiction.

parents. Moreover, they can collect first party analytics data themselves or using a third party, to support the operations of the service and improve it for children under the internal operations exception to the COPPA Rule, as long as that information is used solely for that purpose. In turn, children can engage with appropriate content without being tracked across sites and services, and when permissioned by the parent, utilize other robust features such as sharing and comments with the parent informed and empowered to supervise as the parent deems appropriate. Importantly, because of the Commission's 2013 amendments to the COPPA Rule, children are not banned from child-directed sites and services as a means of operator compliance with the COPPA Rule. Rather, they are assured of an online experience that is COPPA-compliant and a means of securing parental permission to unlock additional features after notice and verifiable parental consent.

However, comments submitted in this proceeding by a group of 31 organizations from the Campaign for a Commercial-Free Childhood to USPIRG detail many new or newly more powerful data collection practices in use in the online environment to deliver advertising and conduct sophisticated analytics. The impact of new practices such as those the parties identified[5] as cross-device identification, ad attribution, persona based advertising, lookalike modeling, user acquisition, audience segmentation, lifetime value, and mediation are not well understood, including by regulators and parents who are making decisions about the permissible collection, use and disclosure of child information, including information designated child Personal Information by the COPPA Rule. These practices raise concerns that industry has the ability to build detailed profiles of child users, including child Personal Information, and perhaps inferred information that when combined becomes very telling, often without parental consent or sufficient disclosure to permit parents to exercise informed parental consent if they are asked to provide it.

Comments by YouTube content creators responding to the recent settlement agreement the Commission and New York Attorney General reached with Google/YouTube[6] concerning collection of child Personal Information on the YouTube platform reveal that many content creators were completely unaware of the existence of the law, which is now more than 20 years old. To the extent those content creators are also parents, this is likely to mean that they have not taken full advantage of the notice and consent procedures that COPPA affords them with respect to their own children. Many of those who are commenting create the wholesome family content that they want to see be available for their own children, and predict that mandating compliance with COPPA on platforms such as YouTube will result in the loss of content for children and livelihoods for those who may have developed businesses on the platform.

Comments submitted in this proceeding, such as those of Jennifer McAllister,[7] reflect perceptions of the COPPA Rule present in the consumer and content creator communities. Ms. McAllister states that she welcomes tracking of her children because she recognizes that behavioral advertising revenue funds the types of family-friendly content she herself creates and that she wants to be available to her children and others. In addition, she feels that the tracking is actually beneficial in that it results in only child content being displayed to her children. Ms. McAllister states that it does not matter to her where her child is exposed to advertising for an item he asks her to purchase, only that he is making the request and further

[5] It should be noted that terminology itself is problematic because there is no agreed upon industry definition of most of these terms or agreed upon terms for these practices.

[6] https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations

[7] https://www.regulations.gov/document?D=FTC-2019-0054-0601

that she would like to be able to engage with content about the child product, especially receiving reviews by other adults of the product. Ms. McAllister is proactive and supervises her children's use of YouTube. She limits her younger children to watching the YouTube child service and employs ad blockers or parental controls at her discretion and feels other parents should have those options, but be free to choose whether to employ them or not.

In terms of the Commission's question regarding benefits and costs as they relate to users and small businesses, such comments portray the COPPA Rule as imposing burdens on parents and small businesses without adequate countervailing benefits. At the present time, the information needed to reach that conclusion, or more importantly to attempt to fine tune this balance to adjust for changes in the marketplace, may be lacking. Nevertheless, such comments articulate some of the tensions that exist or are perceived to exist between child privacy protection, parent empowerment, content creation and ecommerce that the COPPA Rule seek to balance. At the end of the day, COPPA is directed at more than the simple question of whether certain advertisements are appropriate to be shown to children. Inherent in behavioral advertising is the tracking of children across sites and services. And, while advertising revenues in general may underwrite the production of valuable children's content online, the lure of viewing that content where such tracking is present may be injecting children's Personal Information directly into a data economy that lags in its ability to handle this sensitive information.

In light of the concerns raised about the new and more powerful data aggregation tools being employed in the online space discussed above, the building of profiles early in a child's life that are maintained and added to potentially throughout the whole of the child's life is an even greater concern than the content of any specific advertisement shown to a child. Indeed, a major concern advocates have raised is how the online profile created during childhood might affect what content that child sees and how that influences the child's development over the course of his or her entire life. For example, it would be very alarming if childhood pursuits and passions influence what content is made available to him or her as an adult, such as, for example, content designed to influence political behavior or beliefs.

Therefore, the Commission must continue to educate itself, and in turn the rest of the online ecosystem, about these new methods of data aggregation and how a profile started in childhood might affect individuals throughout their lives. Only then can a true cost/benefit analysis be performed. While additional workshops are clearly called for, PRIVO suggests that the FTC establish a standing working group to meet routinely to further this research and understanding.

In Question 2c, the Commission asks what changes can be made to the COPPA Rule to increase its benefits. PRIVO submits that the Commission should encourage industry to cooperate in the adoption of a uniform signal by which a device or browser can give operators notice that the primary user of the device is a child. Operators would then respond by discontinuing any tracking, behavioral advertising, profile building, lookalike modeling or similar data collection practices as well deactivating features that permit a child to potentially disclose Personal Information such as through chat or sharing. Just as commercial casinos in many states are required to maintain a database whereby those who have a gambling addiction can identify themselves to a casino and request the casino's assistance in preventing the addicted person from engaging in certain activities in the casino, so too would parents be able to designate a particular device as one used primarily by a child and secure the operator's assistance in protecting the child's Personal Information. Indeed, because the program would be voluntary, parents could identify whether the device is primarily used by a child under 13 (U13) or a child whose age is between 13 and 18 (U18), thereby assisting operators with compliance in jurisdictions that implement protections for children 13 years of age or older. PRIVO believes that the collection of a persistent

identifier to effectuate such a program would fall under the definition of "internal operations" already present in the COPPA Rule.

B. Overlaps, Conflicts or Perceived Conflicts with other Laws and Regulations

In Question 5, the Commission asks whether there are other laws that conflict with the COPPA Rule and make compliance with one or the other law difficult. PRIVO believes that there are laws that either are in actual conflict or are perceived to be in conflict, leading commenters to blame COPPA for inefficiencies or seek to weaken it for convenience rather than examine and develop innovative alternatives. Two areas PRIVO would like to address are the overlap with COPPA and the Family Educational Rights and Privacy Act ("FERPA") in the US and the overlap of COPPA and foreign privacy regimes such as the GDPR.

As various comments in this proceeding reflect, there is confusion on the part of schools, service providers and parents as to what FERPA and COPPA require, the extent of the protection of the "school official" exemption to FERPA, and what approach to take with respect to clarifying these issues in this proceeding. PRIVO notes that technology can enter a school through different channels, and those differences impact the propriety of having schools provide COPPA consent in the place of a parent.

One channel is where school leadership enters into a contract with a service provider to perform administrative and curriculum functions for the school. Through the contracting process, schools, in theory, should be able to conduct due diligence and negotiate with respect to the issues of third-party disclosure, data retention, data security and use of data to fulfill school reporting obligations or improve the product, and to satisfy themselves and their legal counsel that each of these fits within the FERPA school official exemption. In such a case, PRIVO submits that it would be appropriate that school leadership disclose its use of the vendor's products to parents and provide consent to the vendor in the parent's place, and there is no conflict with COPPA. Further, it could be appropriate for the school to permit service providers to use student data, de-identified if appropriate, in order to improve the product or service because the school or district would do the same if it were providing the service or product using internal resources.

However, there are an increasing number of customizable educational tools, contests (run by non-profits,[8] government and commercial entities alike) and content that are fueled by personal information collected directly from teachers and students and created through use of the service. Schools and teachers are faced with a plethora of ed tech, entertainment and content services. While the service they originally contracted with through the above process may have been compliant, it may thereafter link

[8] While the Commission did not explicitly ask about non-profit entities and its jurisdiction is limited with respect to them, non-profits collect and control large amounts of child personal information. These include traditional youth organizations, athletic programs, and an ever-growing number of enrichment programs operated by foundations that are funded by commercial entities seeking to reach children around STEAM or other educational themes. The Commission should examine whether non-profits share covered information with commercial partners and funders, and require that those commercial entities comply with COPPA due to their knowledge that the information originated with the child-directed activities of the non-profit. In addition, the Commission should examine the extent to which non-profits' privacy policies and marketing materials reference COPPA-like protections, such as statements affirming commitment to the protection of children under 13 and adherence to vague privacy best practices, and consider whether such assertions, which play on the inherent trust parents may have in non-profits, are unfair or deceptive where the entity is not in compliance with COPPA.

students to app stores, platforms and other content that is not. If uses of the product or service by the student is possible in ways that exceed the curriculum or administrative needs of the school, such as to allow the child to continue to use an educational resource over the summer or store/download written assignments after moving into another course or grade, the school can facilitate getting the parent's consent to the "extra-curricular" use of the product, but should not stand in the parent's stead where the use is no longer directly related to the school's purpose. As noted, though, most examples are not this straightforward and making distinctions between "curricular" and "extra-curricular" uses, products and services is becoming blurred. Keeping up with the changes in this market is as overwhelming as in the wider online advertising environment.

Another situation is presented when a pre-existing contract does not exist and the school or teacher simply accepts the online service provider's terms of use. In this case, the school is less able to control issues of data collection, use, storage, security, deletion and sharing. In fact, school leadership may not even be aware that a particular service is in use in its school. Here, it can hardly be said that the individual classroom teacher is empowered by the school to accept those terms of use or that anyone has reached the conclusion that the collection, use, storage and disclosure of student information through this service meets the school's obligations under FERPA, state laws and internal risk assessment parameters. In this context, PRIVO submits that it is not appropriate for individual teachers to stand in the parent's stead and accept the terms of use in reliance on a blanket annual FERPA disclosure. Providers of these types of services should be required to have a separate registration process for those identifying themselves as teachers and not require them to act in a parent's stead without providing evidence of school authorization to do so, which could be through a vouching system, directory, verifiable claim or other means.

COPPA may become the scapegoat for any increased costs of technology use borne by schools or disproportionate impact on the availability of technology for schools in lower income or underserved communities as a result of increased costs. This potentiality only highlights the vital importance of all stakeholders joining together to find ways to first educate schools and individual teachers on the risks to student privacy from unchecked technology use in the classroom. Just as in the YouTube comments noted above, the public perception that if the content is appropriate for children then there is no privacy risk, must be overcome. PRIVO encourages the Commission to review the COPPA education exception to ensure that commercial entities are obliged to verify that the teacher has been given the authority to act on behalf of the school.

Another area of perceived conflict is with child online protections enacted in other jurisdictions. Where an operator operates in multiple countries, it may be required to extend protections to children over the age of 12. However, the Commission should recognize that available technology allows for sophisticated age-gates capable of providing different registration paths based on age and jurisdiction.

Rather than view these differences in the regulatory schema as conflicts, PRIVO believes that there are many positive elements of other laws that the Commission could look to in its review of COPPA which, if incorporated, would enhance COPPA's protections and provide a more unified regulatory framework for operators. For example, GDPR calls for special protections for children above the age consent, which can be up to 17.[9] As noted above, establishing a voluntary means for operators to engage with children 13 to

[9] Individual countries can establish different ages of consent.

17 would satisfy many of the issues commenters in this proceeding view as conflicts. The GDPR also requires that privacy settings initially be set to a high level that the user can than change. Moreover, GDPR requires just in time educational notices/disclosures on what it means to change the settings. That high level includes requiring the user to opt into tracking that does not fall under the support for internal operations exception, and the ability to toggle to an opted-out position to revoke consent to tracking.

One aspect of the GDPR that the COPPA Rule should mirror is in establishing a child's rights, as distinguished from the rights of the parent in relation to the child, which is what COPPA addresses. The GDPR is very clear that the child has the same rights as a data subject at or above the age of consent to, for example, erasure of their personal data. Additionally, a child approaching the age of consent must receive notice that at the age of consent the child will become responsible for managing the online permissions previously granted by their parents. Currently, under COPPA, there is no similar required mechanism. Based on this, PRIVO would also recommend that the FTC look to the approach of the UK data protection authority, particularly of the Information Commissioner's Office Age Appropriate Design Code which will come into the force early in 2020. The Code requires age appropriate notice to children and privacy by design and default.

II. Definitions

What constitutes a child directed online service needs no clarification, and exceptions to parental consent are sufficient. However, rebutting the presumption that child directed content is only viewed by children is critically important for educators and parents who view content. This would allow for users to be treated differently according to age (mixed audience definition). Child directed content could therefore default to a non-COPPA triggering feature set and the user who has reached the age of consent could prove age or role and exercise their right to be treated as a teen or adult. However, as disruptive as it may be, users will have to be treated as children until the age is known at which point a user 13 or older can be treated differently.

Services not targeted to children that have large numbers of children must be addressed as it can result in online harm to the child due to the inherent privacy and safety risks. General audience services with large numbers of children should be required to implement COPPA protections by providing a restricted service for these users and/or seeking parent consent for use. Without the requirement to implement special protections these services have and are exposing children to online harms. If the service is directed to a general audience and not targeting children, then robust age gates or alternative methods must be employed to prevent access. Clear criteria of what targeting children means is needed, including a review of marketing materials both internal and public and audience demographic information. Also, thresholds for number of child users at which COPPA protections must be provided should be more clearly defined, along with how actual knowledge is proven (or not).

The 2013 changes to the definition of a child directed service that does not target children as a primary audience have been positive for children. These changes allow the use of an age screen, resulting in better protections for children where the service employs a compliant neutral age gate and thereby restricts certain collection and use of personal information or seeks parent consent for collection and use. Currently, guidance is widely ignored resulting in a child circumventing the age gate. The requirements should be prescriptive to help resolve the issue of gaming of age gates which then results in

tens of thousands of child accounts on inappropriate and unsafe social media platforms and other such services. Age gates should be required to collect a freely given date of birth, if year of birth is collected the age gate must screen for 13 and under, not 12, which commonly occurs. A session cookie must be dropped to prevent the child from returning and entering an inflated date of birth. The user should not be able to back button, refresh and add a different age. If the service is an app, the user should not be able to change the age entered. The only way that age could be changed is if the user were to delete the app and download it again entering different details. If the service collects and processes personal data that would be considered high risk, i.e. public sharing of images, video, free text and communications, then age gates are not robust enough of a mechanism and a secondary authentication level should be required.

The Commission asks whether the definition of personal information should include inferred information about children. The COPPA Rule's definition of personal information should not be expanded to include information that is inferred about children, unless combined with other personal information. Such an inclusion would create significant uncertainty around the scope of the COPPA Rule and potentially stifle the development of new products and services. For example, contextual advertising, which is explicitly permitted under COPPA[10] and is often held up by privacy advocates as a viable alternative to targeted advertising because it does not require the collection and use of personal data, instead using contextual clues to share relevant ads. If the Commission were to include inferred data in the definition of personal information, it likely would have the unintended effect of prohibiting contextual advertising.

The definition of support for internal operations has been valuable to children and to business. It allows for the use of a third party to perform a task the operator cannot do effectively or cost efficiently. It also provides that personal information cannot be shared onwards by the third party. Nevertheless, the definition is open to abuse. For example, the Commission should make clear whether attribution and remarketing can be claimed to be support for internal operations. In PRIVO's experience, measures can be taken to provide a compliant version of attribution services, but most providers are not.

III. Provisions Regarding Safe Harbors

In Question 29, the Commission asks about the overall efficacy of the Safe Harbor program, whether there should be any modifications to Safe Harbor approval, monitoring or transparency, and whether there should be any modifications made to the language of the COPPA Rule that addresses the Commission's discretion to initiate an investigation or bring an enforcement action against an operator participating in a safe harbor program. PRIVO submits that, properly operated, a Safe Harbor does invaluable work in bringing members into compliance, educating members and other stakeholders as to the important issues involved in children's online privacy protection, and in so doing, frees Commission staff to focus scarce investigative and enforcement resources on those operators that may not be striving for compliance.

Nevertheless, PRIVO is aware that in a few instances, operators have refused to take steps prescribed by a Safe Harbor, and then tried to join another Safe Harbor in the hopes of not being asked to take those same steps. These rare occurrences waste Safe Harbor resources, seek to create competition among the Safe Harbors on the issue of compliance, and if left unaddressed, could undermine confidence in one or

[10] 16 C.F.R. 312.2 (Definition of "support for internal operations").

more Safe Harbors or the program as a whole. Where PRIVO has encountered companies shopping for the best compliance response, it has turned those companies away. Accordingly, PRIVO is calling for each Safe Harbor, as part of its intake procedure, to ask the potential new member whether it is subject to any investigations and, further, whether it has previously been advised by a Safe Harbor to take steps and failed to do so. Similarly, where Safe Harbors have questions or disagreements as to the privacy practices of a member of another Safe Harbor, they must notify the other Safe Harbor and the FTC confidentially so that the Safe Harbor program as a whole can be informed by the dialogue around the issues and consistent approaches can be maintained.

With respect to Safe Harbor approval and monitoring, it is appropriate for the Commission to require the Safe Harbor to demonstrate current skill sets and experience adequate to administer a robust and up to date program. Programs must also be able to show that they have members with child directed services in order to maintain Safe Harbor status. An entity's status as commercial or not for profit has no bearing on its integrity or ability to provide robust compliance services. What ensures a Safe Harbor is equipped to carry out its role is working closely not just with members, but with industry in general, at a grass roots level, to ensure comprehensive understanding of all areas of this evolving and dynamic environment. An example might be the ability to run packet sniffing tools and analyse the results to uncover third party tracking and any potential violations.

While Safe Harbor remains a neutral third party, any competition between the Safe Harbors should be on added value and support that is provided at a service agreement level only. The FTC requires the resources not only to ensure that a Safe Harbor is meeting and enforcing its own requirements, but also to work closely with the Safe Harbors on a more frequent and regular basis to share learnings of the work taking place and to help keep pace with the fast evolving developments in children's content, services and for example the ad industry. Similarly, there may be areas where the FTC and Safe Harbors can bring more transparency into the program as whole, such as the release of aggregate numbers of sites or services covered by the program. It is vitally important, however, that all parties to the process appreciate that the members of the Safe Harbor programs are among the most proactive in their compliance efforts and provide valuable insights that benefit the Safe Harbors and the FTC overall. Therefore, transparency efforts must protect the confidentiality of the members, to demonstrate the absolute value of participation in a Safe Harbor.[11]

Finally, with respect to the language of Section 312.11(g), PRIVO submits that the section is internally contradictory. The first sentence relieves operators of any liability for a violation of COPPA if they are participating in an approved self-regulatory program. The remainder of the section confuses the section's message. Should the Commission have concerns with the compliance of an operator, it should bring those concerns to the Safe Harbor. If it is determined that corrective action is necessary, the Safe

[11] Only a relatively small percentage of companies are in Safe Harbor. This does not create a level playing field for industry. Safe Harbors provide an invaluable service for business in the children's online space and for others that may attract children. Those who join a Safe Harbor should not be penalized for going the extra mile.

Harbor should assure that the operator takes it. This has been the Commission's practice, and that practice does not seem to be influenced by the remaining language of the Section.

PRIVO is pleased to have had the opportunity to bring these issues forward and looks forward to working with the Commission on these and similar issues going forward.

Respectfully submitted,

PRIVACY VAULTS ONLINE, INC. d/b/a PRIVO

By: ___/s/_____
Denise Tayloe, CEO
Claire Quinn, CIPP/e, VP Compliance