Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

In the Matter of	)	
	)	
Implementation of the	)	Docket No. 339
Children's Online Privacy Protection Rule	)	Project No.P104503

COMMENTS OF
CENTER FOR DEMOCRACY & TECHNOLOGY

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the Commission's proposed revisions to the Children's Online Privacy Protection Rule. The Commission discusses a number of recommendations for changes to the COPPA regime in the Proposed Rule. The Commission properly rejects some of the recommendations, including suggestions from other commenters to expand COPPA's scope to cover older minors or general-audience websites, and makes a number of proposals that will bring COPPA up-to-date and provide parents with better information and assurances about whether and how their children's personal information will be collected. Some of the proposed revisions, including changes to the definition of "personal information", raise significant technical and implementation questions that the Commission must address before adopting the revised Rule. The Commission also proposes a highly problematic new method of obtaining parental consent that we respectfully ask the Commission to reconsider.

I. In general, the Commission's proposals keep the COPPA Rule focused on protecting children's privacy.

a. The Commission appropriately maintains the age range covered by the Rule at children under 13.

While several commenters suggesting expanding COPPA to cover older minors, the Commission rightly noted that applying the parental notice and consent model to teen users "would be less effective or appropriate", citing older minors' "right to access information and express themselves publicly."[1] The Commission also discussed the practical difficulty in expanding COPPA to cover websites "directed to teens", noting that doing so "might unintentionally burden the right of adults to engage in speech online."[2]

CDT is also pleased to see the Commission's recognition of the need for stronger privacy protections not just for older minors, but for all users. We agree with the Commission that "it is essential that teens, like adults, be provided with clear information about uses of their data and be given meaningful choices about such uses" and look forward to working with the Commission as it explores "new privacy approaches that will ensure that teens — and adults — benefit from stronger privacy protections than are currently generally available."[3]

---

[1] Federal Trade Commission, Children's Online Privacy Protection Rule, Proposed Rule, 76 Fed. Reg. 187, 59805 (Sep. 27, 2011)(hereinafter "Proposed Rule"), *available at* http://ftc.gov/os/2011/09/110915coppa.pdf.
[2] *Id.*.
[3] *Id.*

b. The Commission is right to retain the "actual knowledge" standard for operators.

The Commission also rejects suggestions by a number of commenters to broaden COPPA's scope by including sites that have a general idea, or "constructive knowledge", that some of their users are children. Changing the Rule's knowledge standard in that way would pull many of the most popular user-generated content and social networking sites within COPPA's ambit, requiring them to collect more information from *all of their users* in order to determine which users were children whose personal information is covered by COPPA, and which were not. As the Commission recognizes, this would encroach on adults' and minors' rights to access and post information anonymously, and would lead to exponentially more data collection — an ironic outcome for a privacy protection law.[4]

CDT applauds the Commission's retention of the statutory "actual knowledge" and "directed to children" standards, and its concomitant recognition that COPPA "was never intended to apply to the entire Internet, but rather to a subset of websites and online services."[5] As the Commission notes, actual knowledge is a far more workable standard that provides greater certainty to website operators,[6] and the Rule's definition of "personal information", particularly if revised as proposed, "might prove infeasible if applied across the entire Internet.

c. The Commission proposes a number of revisions that will bring COPPA up to date and better protect children's privacy.

CDT is pleased to see the Commission's proposals for incorporating a number of privacy-protective principles into the COPPA Rule. We are especially pleased to see that the Commission has embraced the full range of the Fair Information Practice Principles. The Commission's decision to include a data minimization provision,[7] for example, will help ensure that information about children is not kept for excessively long times and will thereby reduce the risk of accidental data breach or inappropriate use of that information. We further applaud the Commission's careful attention to security practices. We support both its inclusion of security considerations in its data deletion requirements[8] and its sensible requirement that third-party operators put in place reasonable security procedures.[9] The Commission has wisely recognized that a piece of data is only as secure as the "weakest link" amongst all the operators that hold it. However, consistent with the Commission's goal of addressing business-to-business data sharing, the Commission should make it clear that these additional data security requirements apply only to other FTC-regulated entities with which the operator has a contractual relationship.

We also applaud the Rule's updated notice requirements.[10] The Commission has wisely recognized that long, obtuse privacy policies offer little useful guidance for parents (or others) who are trying to understand online data flows. We believe that the Commission's emphasis on clearly labeled, prominently located, "just in time" notices that contain meaningful information

[4] *Id.* at 59806; *see also* Center for Democracy & Technology, Supplemental Comments in COPPA Rule Review (July 2011), *available at* http://cdt.org/files/pdfs/CDT_Supplemental_Comments.pdf.
[5] Proposed Rule at 59806.
[6] *Id.*.
[7] *Id.* at 59822 (revision to16 C.F.R. §312.10).
[8] *Id.*
[9] *Id.* at 59821 (revision to §312.8).
[10] *Id.* at 59814-16 (revision to §312.4).

will promote parental understanding of online operators' privacy practices.

The Commission also seeks to strike a better balance between protecting children's privacy and enabling their use of interactive sites and services by altering the so-called "100% deletion standard" for operators who allow children to post information publicly.[11] This proposal, which would exempt from the definition of "collection" instances where operators take reasonable measures to delete all or virtually all of a child's personal information before a post goes public, still places a high priority on keeping children's personal information private but recognizes that the perfect-deletion requirement placed too high of a barrier for risk-averse operators.

II. Several of the proposed revisions to the definition of personal information require further clarification from the Commission.

a. The proposed inclusion of IP address and other persistent identifiers in the definition of personal information raises technical and implementation questions that must be answered before the revised definition can be adopted.

The Commission proposes amending the definition of personal information to include "[a] persistent identifier, including . . . an Internet Protocol (IP) address . . . where such persistent identifier is used for functions other than or in addition to support for the internal operations of, or protection of the security or integrity of, the website or online service." CDT has long advocated for comprehensive privacy regulations that include IP address as personally identifiable information (PII) and that regulate the collection and use of PII. However, we have also recognized that blanket prohibitions on collection are sometimes impractical and counterproductive, and that in certain instances, collection should be allowed but subsequent use limited (see CDT's draft definition of "Do Not Track"[12]). With regard to the COPPA Rule, CDT cautioned the Commission in our 2010 comments that, because of the Rule's prohibition on the collection of personal information from children without prior parental consent, including IP address as COPPA-covered personal information would present a practical impossibility for operators of first-party sites: an operator of a website directed to children would "collect" personal information the very first time a child attempted to access the site, providing the operator with no opportunity to comply with COPPA and obtain prior verified parental consent.[13]

CDT is pleased to see that the Commission's proposal tries to balance both the technical and potentially identifying aspects of IP address. By limiting the treatment of IP address and other persistent identifiers as personal information to when they are used for purposes other than maintaining the functionality or security of the site or service,[14] the Commission has drawn an

[11] *Id*. at 59808.
[12] Center for Democracy & Technology, What Does 'Do Not Track' Mean?: A Scoping Proposal by the Center for Democracy & Technology, Version 2.0 (April 27, 2011), *available at* http://www.cdt.org/files/pdfs/20110447_DNT_v2.pdf.
[13] Center for Democracy & Technology, Individual Comments in COPPA Rule Review 7-8 (June 2011), *available at*http://cdt.org/files/pdfs/CDT_Individual_Comments.pdf.
[14] The proposed definition of "support for the internal operations of the website or online service" is "those activities necessary to maintain the technical functioning of the website or online service, to protect the security or integrity of the website or online service, or to fulfill a request of a child as permitted by §§312.5(c)(3) and (4), and the information collected for such purposes is not used or disclosed for any other purpose." The Commission develops this definition in the text of the Rule Review, stating that "[t]he new language would permit operators' use of persistent identifiers for purposes such as user

appropriate line between functional uses of persistent identifiers and those uses which may threaten children's privacy.

The proposed revision does, however, require further clarification. With the inclusion of IP address and other persistent identifiers typically transmitted by a user's browser, a new range of operators potentially face obligations under the Rule. COPPA has traditionally covered the activity of first-party site operators accepting data input from users (usually through forms or interactive fields), some of which might be personal information covered by COPPA. Including data such as IP address and device identifier in the list of personal information will more directly implicate operators of online services such as analytics providers and advertising networks that run as third parties on websites and online services targeted to children. These operators routinely acquire this type of data from users, often without any obvious direct interface with the user.

CDT believes that it may be appropriate in some circumstances for these operators to have independent obligations under COPPA; however, because they do not typically provide forms for users to input data such as age or date of birth, these entities are unlikely to meet COPPA's actual knowledge standard. Moreover, unless these third-party services themselves are purposefully directed at children (as opposed to a general audience), we do not believe that these services should be deemed "directed at children" merely because the sites they service are themselves directed at children. Instead, the responsibility for disclosing information sharing and obtaining parental permission should lie with the first-party.

Under the Rule's current definitions, it is unclear whether and how COPPA applies to the analytics services, advertising networks, market researchers, widget providers, and other operators of online services that either do not typically interface directly with users or are designed to be incorporated into a first-party site without direct knowledge or express consent by the provider of the service (for example, a social plugin).

In the case of analytics providers, for example:

- An analytics provider might offer information about how a user navigates an operator's site — and only that operator's site; in this case, the analytics provider seems to fall under the Rule's definition of *third party*.[15]
- An analytics provider that correlates user activity across multiple sites would almost certainly be considered a first-party operator under the Rule.[16]

---

authentication, improving site navigation, maintaining user preferences, serving contextual advertisements, and protecting against fraud or theft." Proposed Rule at 59812.This definition is appropriately narrow and permits truly functional uses of persistent identifiers without leaving loopholes regarding data processing that could be exploited.

[15] 16 C.F.R. §312.2 (defining *third party* as "a person who provides support for the internal operations of the website or online service and who does not use or disclose information protected under this part for any other purpose").

[16] 16 C.F.R. §312.2 (defining *operator* as "any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes . . . ."). *See also* Proposed Rule at 59812 ("[A]n advertising network or analytics service that tracks a child user across a set of sites or

Similar questions arise for each type of non-user-facing entity that could collect children's personal information in the form of IP address: When are these entities themselves *operators* under the Rule? When are they considered *directed to children*? And when do they face their own obligations to provide notice and obtain verified parental consent prior to collecting a child's information? Clear answers to these questions from the Commission will help avoid chilling innovation in sites and services designed for children.

It may be the Commission's intention to keep the bulk of the notice and consent obligations on the traditional operators of user-facing websites and online services that are aimed at children. For example, the Commission proposes a revision to the notice obligation that appears to designate these first-party operators as the responsible party for providing notice and obtaining consent for data collection, use, and disclosure by service providers that might have access to a child's personal information through the first-party operator's site.[17] This makes intuitive sense: the operator of the website is in the best position to interact with the child and her parent, to know that his own site is directed to children, and to provide information about the data collection and use practices of the third-parties that he allows onto his site (as is required under the proposed revision). Keeping the parental consent obligations on traditional operators will also minimize the amount of *parents'* personal information that must be collected as part of the consent verification process.

This should be the case even if the first-party operator does not itself collect personal information from its users beyond what is necessary to support the internal operations of the site; if a site directed to children permits service providers to collect personal information about its users, it must provide clear notice and obtain parental consent first. (However, the first-party operator's obligation should be limited to accurate identification of these entities and reasonable disclosure of their data collection and use practices, as the Commission proposes; the revised notice provision in §312.4 should not be read to assign liability to first-party operators for the actions of these entities to the extent they vary from the entity's disclosed practices.)

Operators of analytics services, advertising networks, and social plugins that do not intentionally target their services to children should not have independent COPPA notice and consent obligations simply because a site directed to children has chosen to use their service. As discussed above, operators of these general-purpose services are unlikely to ever obtain actual knowledge that a particular user is a child. Many of these operators, including providers of social plugins and embeddable media content, provide their services free of charge and without much meaningful contact with the first-party operator. If these operators could find themselves facing COPPA compliance obligations simply by virtue of offering their services in conjunction

---

services, but stores this information in a separate database rather than with the persistent identifier, would be deemed to have collected personal information from the child under this proposed paragraph.").

[17] Proposed Rule at 59815 (revising §312.4(b) and accompanying text). While we have argued that first parties should be able to obtain permission for transferring information to service providers with which consumers do not have direct interaction, the Commission should consider whether there are circumstances under which first-party platforms (such as operating systems, browsers, and mobile devices) should be able to obtain blanket consent for other first parties (such as websites or applications). Those new first parties are better situated to obtain their own consent from parents, but there may be a benefit to allowing parents to give one-time consent on platforms that they trust provided there is meaningful notice and control for parents going forward. CDT has not adopted a final position on this issue.

with a clickthrough agreements, these operators would likely refuse to do business with sites directed to children or with sites generally, out of fear that a COPPA-covered site might place the widget or content on its site and thereby expose the service provider to independent COPPA-compliance obligations.[18]

However, if the non-user-facing entity takes steps to target a portion of their service to children — if, for example, a behavioral advertising network includes "under 13" as a potential classification in a user's profile — then they should reasonably expect that they will incur their own independent COPPA notice and consent obligations.[19]

b. The Commission should warn operators and COPPA safe harbor programs about the risk for inadvertent disclosure of a child's user ID or screen name based on site architecture.

The Commission also proposes to add to the definition of "personal information" "(d) A screen or user name where such screen or user name is used for functions other than or in addition to support for the internal operations of the website or online service." CDT agrees that usernames and screen names can often identify an individual: particularly when users employ the same screen name across sites, whether it is a version of the user's full legal name or a pseudonym, there is significant opportunity for operators to track or correlate an individual's behavior across multiple websites, without the user's knowledge. The Commission appropriately recognizes this potential impact on children's privacy with the caveat that usernames are considered 'personal information' only when used for purposes beyond the internal operation of a site or service.

Because the Rule also regulates the disclosure of children's personal information, the Commission should consider providing guidance to operators of sites or online services directed to children about the issue of referrer URLs. Depending on how operators structure their websites, there is a risk that screen names, usernames, and other unique user identifiers may be disclosed to third parties as a user navigates within the site or follows a link to a third-party site.[20] Indeed, this was one of the issues the Commission addressed in its recent settlement

[18] Jim Brock, "Developer alert: Flurry analytics adopts new child privacy rule", Privacy Choice (Oct. 25, 2011) *available at* http://blog.privacychoice.org/2011/10/25/developer-alert-flurry-analytics-adopts-new-child-privacy-rule/.

[19] If the Commission anticipates that behavioral advertising networks could incur their own COPPA obligations in this manner, then it should clarify its comment in the Rule Review that the "support for internal operations" exemption for preliminary collection of a user's IP address does not apply to behavioral advertising networks. ("[T]he new language would require parental notification and consent prior to the collection of persistent identifiers where they are used for purposes such as amassing data on a child's online activities or behaviorally targeting advertising to the child. Therefore, operators such as network advertisers may not claim the collection of persistent identifiers as a technical function under the "support for internal operations" exemption." Proposed Rule at 59813.) Operators of behavioral advertising networks cannot claim that all of their activity fits into the "internal operations" exemption *for the first-party site*, but these operators would need to be able to 'collect', users' IP addresses in order to provide notice and obtain consent. See CDT Individual Comments *supra* note 13.

[20] *See* Justin Brookman, "Why Facebook Apps Story Is a Problem for Entire Web", CDT Policy Beta (Oct. 19, 2010), *available at* http://www.cdt.org/blogs/justin-brookman/why-facebook-apps-story-problem-entire-web;Jonathan Mayer, "Tracking the Trackers: Where Everybody Knows Your Username," Stanford Law School Center for Internet and Society (Oct. 11, 2011), *available at* http://cyberlaw.stanford.edu/node/6740.

with Facebook.[21] Because the privacy concerns at issue here may not be immediately apparent to developers of websites and online services, the Commission should highlight this potential issue for operators and for COPPA safe harbor programs so that they can be sure to structure their sites to avoid inadvertent disclosure of children's screen names or usernames to third parties.

c. Because only personal information about a specific child can be properly included in COPPA's parental consent process, the Commission should revise its proposed addition of photographs and other media to specify that only media depicting the particular child user is included in the definition of personal information.

The Commission also proposes revising the Rule's treatment of photographs as "personal information," expanding from the current definition's inclusion only of "a combination of a . . . photograph of the individual with other information such that the combination permits physical or online contacting."[22] However, the Commission's proposed language, "A photograph, video, or audio file where such file contains a child's image or voice,"[23] is too broad. The stipulation "where such file contains *a* child's image or voice" appears to apply to a photo, video, or audio file of any child — in contrast to the current definition, which explicitly applies to a "photograph of the individual." COPPA only rationally works as a requirement on operators to obtain consent from the parent of *a particular* child before collecting personal information about that child (as uploaded by that child). It cannot be broadened to attempt to regulate the uploading of photographs of *any* child, as this would raise significant practical and constitutional challenges. The Commission should make clear in the final Rule that the definition applies to media files to the extent they feature the child who uploads them — the child for whom the parent can reasonably give consent.

The Commission is correct that images and audio recordings can used to identify individuals with increasing accuracy, and that this development raises privacy issues for children as well as adults. The question of how to protect individuals' privacy from others' actions — how to respond to users who upload photos of their friends — is likewise a difficult one to answer. Biometric information is used in a variety of commercial contexts — offline and online — that extend well beyond the bounds of COPPA.[24] The privacy issues raised by the spread products and services based on facial recognition and detection, for example, are complex and difficult to resolve through regulation without suppressing innovation, overstepping constitutional boundaries, or turning many businesses and consumers into criminals.

CDT believes the most effective way to protect the privacy of children in the context of biometric identification is through the combination of a baseline consumer privacy law and enforceable industry codes of conduct.[25] The laws and codes must cover uses of biometric information and also address the privacy of children in multiple contexts. In fact, some industry codes of conduct already prohibit the use of facial recognition and detection to identify children in retail

[21] *See* Federal Trade Commission, Complaint in the Matter of Facebook, File No. 092 3184, ¶¶ 37-40, *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf.
[22] 16 C.F.R. §312.2.
[23] Proposed Rule at 59813.
[24] *See* Center for Democracy & Technology, Seeing Is ID'ing: Facial Recognition and Privacy (Dec. 2011), *available at* http://cdt.org/comments/seeing-id%CA%BCing-facial-recognition-privacy-cdt-comments-advance-ftcs-workshop-facial-recognit.
[25] *Id*.

settings,[26] and some companies configure their facial recognition and detection systems to ignore children under 13.[27] COPPA regulations should have a role in protecting child privacy with regard to biometric identification, but the Commission should craft that role in relation to the roles of Congress, industry, and other federal agencies. CDT therefore recommends that the Commission undertake a more thorough inquiry into how COPPA should address privacy concerns related to the biometric identification of children. CDT recommends that the Commission coordinate this inquiry with existing efforts to explore the privacy issues associated with facial recognition and detection, such as the process already underway at the Federal Trade Commission,[28] as well as the Department of Commerce's multi-stakeholder process to promote industry self-regulation.

d. The Commission should adopt the proposed addition of geolocation information and provide guidance to operators and COPPA safe harbor programs to help them avoid inadvertent collection of geolocation information.

CDT commends the Commission for including geolocation in its proposed definition for personal information. In recent years, the accuracy of location data has improved while the expense of calculating and obtaining it has declined. For example, digital cameras or mobile devices frequently "geotag" photos with latitude/longitude-coordinate metadata (called Exif data),[29] and mobile platforms provide developers with convenient application programming interfaces (APIs) to determine the device's current location.[30] When linked to other information or identifiers (such that it can be collected over time), geolocation data can reveal highly specific personal information about a child's habits and location, including identity and/or a probable place of residence.[31] It is now a technically trivial to convert (for example) a latitude and longitude into a street address, which, when associated with data points (for example, timestamps that indicate that this is the street address where the child spends her evenings) could then be used to contact an individual.[32] Inclusion of this sort of geolocation under the Rule will help to achieve COPPA's goals.

However, given this ubiquity of location information, we are concerned that good-faith operators might become inadvertently noncompliant. For example, the operator of a website directed to children that allows images to be uploaded but lacks the capability to detect or strip Exif data

[26] *See, e.g.,* Digital Signage Federation, Digital Signage Privacy Standards, *available at* http://www.digitalsignagefederation.org/standards.
[27] *See, e.g.,* Dale Buss, "Jell-O Tempts Adults (Kids Not Allowed) With Intel Face Recognition, BrandChannel (Dec. 21, 2011), *available at* http://www.brandchannel.com/home/post/2011/12/21/jell-o-temptations-machine-122111.aspx.
[28] Federal Trade Commission Workshop, "Face Facts: A Forum on Facial Recognition Technology," December 8, 2011, http://www.ftc.gov/bcp/workshops/facefacts/.
[29] Robert Vamosi, "What Your Digital Photos Reveal About You", PCWorld (Sep.12, 2010), *available at* http://www.pcworld.com/article/205296/what_your_digital_photos_reveal_about_you.html
[30] Scott Thurm and Yukari Iwatani Kane, *Your Apps are Watching You*, THE WALL STREET JOURNAL, December 17, 2010, *available at* http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.
[31] A study by Microsoft research showed that using GPS tracks from a vehicle and heuristic algorithms made identification of home location possible. John Krumm, Interference Attacks on Location Tracks, Proceedings of the 5th International Conference on Pervasive Computing 127 (2007), available at http://research.microsoft.com/enus/.
[32] *See, e.g.,* The Google Geocoding API, http://code.google.com/apis/maps/documentation/geocoding/.

from uploaded photos may unknowingly collect a child's personal information (as imbedded in the image's Exif data). Stripping geolocation from images once they reside on the operator's server is certainly possible, but will not necessarily be intuitive or technically simple for a small site operator to implement. We suggest the Commission release further guidance, targeted at developers and COPPA safe harbor programs, to help good-faith operators ensure compliance with the Rule.

III. The Commission should be careful about endorsing the use of government-issued IDs as online identifiers and authenticators.

The Commission proposes to allow operators, in obtaining verified parental consent, to verify a parent's identity by checking a form of government-issued identification.[33] The proposal would require operators to delete this information promptly after completing verification, which would help to allay concerns about possible data breach of rich records of identifying information about parents. However, two other concerns need to be addressed: (1) The use of government IDs as an online identifier, and (2) the risk of normalizing requests for government-issued identification such as Social Security Numbers or driver's license numbers by websites, which would diminish users' alertness against phishing scams and identity theft.[34]

On the first issue, we urge the Commission to emphasize that it is not endorsing – indeed, that it opposes – the use of government-issued identifiers as online identification for non-government websites. The Commission needs to make it crystal clear that a government-issued ID should not be used in whole or part as an online ID for non-governmental websites and should not be included in whole or part in any username-password combination or in any other type of online identifier for non-governmental websites.

In addition, the Commission should make it clear that it is not in any way supporting the use of government-issued ID numbers for age verification purposes. The issue here is verifying the identity of the parent for consent purposes, not verifying the age of any user. The problems of online age verification have been widely documented.[35] In 2009, after 10 years of tortuous litigation, including two Supreme Court decisions, the Child Online Protection Act was conclusively struck down when the Supreme Court declined to hear the government's appeal of the Third Circuit's third opinion on the case, upholding a permanent injunction against enforcement of the law because of Constitutional problems, including problems associated with online age verification in First Amendment contexts. The Commission should be very careful to specify that it has no new information and no new views on the question of online age verification.

---

[33] Proposed Rule at 59818 (proposing to revise §312.5(b)(2) to include "verifying a parent's identity by checking a form of government-issued identification against databases of such information, provided that the parent's identification is deleted by the operator from its records promptly after such verification is complete.").

[34] According to the Commission's own estimates, "as many as 9 million Americans have their identities stolen each year." Federal Trade Commission, Fighting Back Against Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

[35] "Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force" (Dec. 2008), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf.

The second area of concern relates to verification or authentication. Online identity verification or authentication, of course, remains a major challenge for the Internet. As the Commission has recognized, the Social Security Number functions very well (too well, in some ways) as an identifier, but its use as an authenticator is more complicated, because it is only a quasi-secret.[36] Public policy has been conflicted on the use of the SSN, although recent policy efforts have focused on reducing exposure of the SSN.[37] Both the Commission and participants in the Internet ID and security eco-systems must be careful to ensure that more widespread use of the SSN as an authenticator does not diminish its value for that very purpose, as consumers disclose it to more and more online entities. The Commission recognizes that driver's license, Social Security Number, and other information on government-issued identification are typically considered to be sensitive data.[38] And in other settings, the Commission has cautioned consumers to be suspicious of websites or emails that ask for sensitive information.[39] The Commission needs to be careful to ensure that, by allowing the use of government IDs for identity verification purposes in the COPPA context, it is not encouraging practices that reduce consumers' sensitivity to security risks

* * *

We appreciate the opportunity to comment on the Commission's proposed revisions to the COPPA Rule, and we look forward to working further with the Commission as it continues its review.

Respectfully submitted,

/s/

Justin Brookman
Emma J. Llansó
Center for Democracy & Technology
1634 I Street, NW, Suite 1100
Washington, DC 20006
(202) 637-9800
jbrookman@cdt.org
ellanso@cdt.org

December 23, 2011

[36] Federal Trade Commission, "Security in Numbers: SSNs and ID Theft" (Dec 2008) http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf.
[37] The most recent federal statute seeking to limit use of the SSN is the Social Security Number Protection Act of 2010, PL 111-318. For a history of recent efforts to rein in use of the SSN, see Privacy Rights Clearinghouse, "Fact Sheet 10: My Social Security Number – How Secure Is It?" (rev. Aug. 2011) https://www.privacyrights.org/fs/fs10-ssn.htm.
[38] Proposed Rule at 59818 n.141 and accompanying text.
[39] *See, e.g.*, OnGuardOnline.gov, Avoiding Online Scams, http://onguardonline.gov/articles/0001-avoiding-online-scams; Phishing, http://onguardonline.gov/articles/0003-phishing.