Comments of
Berin Szoka, President
TechFreedom[1]

on
Children's Online Privacy Protection Act (COPPA) Rule Review

Before the Federal Trade Commission[2]
December 23, 2011

What do we want the Internet to offer children? The following top ten values should guide the FTC's current COPPA revisions, and inform any future re-examination of COPPA by the agency or Congress:

1. **Power of Parental Control**. Parents should have the opportunity, and means, to decide how much sharing of personal information based on their own values and judgments about privacy, safety and exposure to marketing. This control should scale with the childhood development states. Ideally, parents should be able to tailor their children's experience beyond making binary decisions about whether to authorize a site or service.
2. **Simplicity of Parental Control**. Parents should be able to exercise such control as easily as possible.
3. **Privacy & Security**. While it might seem obvious that COPPA should enhance, rather than undermine children's privacy and the security of data collected about children, COPPA could, if revised imprudently, result in the collection of *more* data about children, and increase the risk of exposing that data to those who might mis-use it.
4. **Education & Citizenship.** Digital media should offer children a vehicle for developing as informed citizens of an information society and economy. Using sites and services appropriate for their developmental maturity ensures that they will be well-prepared later on in life, and that our educational system can make effective use of digital tools.
5. **Expression**. Digital media should empower children to express themselves, subject to parental control.
6. **Abundance**. Digital media should be abundant, much like the broader Internet.

---

[1] Berin Szoka is President of TechFreedom, a non-profit, non-partisan technology policy think tank. He has written and commented extensively on COPPA. In particular, he testified on COPPA before the Senate Commerce Committee on April 29, 2010, available at http://tch.fm/syexUo, ("Szoka Testimony") and is the author, with Adam Thierer, of *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech* (June 2009) ("COPPA 2.0"), available at http://tch.fm/rAhJbf.

[2] COPPA Rule Review, 16 CFR, Part 312, Project No. P104503 ("NPRM").

7. **Diversity**. Digital media should be diverse, much like the broader Internet.
8. **Affordability**. Digital media should cost as little as possible without compromising quality.
9. **Innovation**. Digital media should, like the rest of the web, constantly improve in quality, sophistication, and interactivity.
10. **Competition**. Competition in digital media and low barriers to entry will promote abundance, affordability and innovation.

Unfortunately, some of the changes proposed by the FTC in the name of promoting parental control, privacy and security might, despite their noble intentions, make choice more difficult, while also driving up prices, reducing the quality and quantity of children's content, and diminishing competition. There is no free lunch, even when it comes to children's content.

If COPPA is to aid parental authority effectively, while promoting these other values in children's digital media, the FTC must carefully consider the unintended consequences of revising COPPA. In particular, the FTC should:

1. **Retain email plus** as a mechanism for verifying parental consent, or at least:
    a. Avoid subjecting network and platform operators to more burdensome consent requirements; and
    b. All data collected under previous standards will be "grandfathered in" such that no new consent need be obtained.
2. Consider holding a public workshop on **alternative mechanisms for verifying parental** consent.
3. Consider how to **promote the development of consent management platforms** by which operators of platforms that support other applications and services can obtain consent on behalf of those third parties for strictly limited purposes.
4. **Not include persistent identifiers in the definition of personal information**, or at least:
    a. Add an exception in paragraph (h) equivalent to that in paragraph (g): internal uses of information gathered using a persistent identifier may be gathered and used within an analytics or advertising platform without requiring parental consent;
    b. Clarify that no platform shall be considered an operator subject to COPPA (thus needing recourse to such a definition exception in the first place) by virtue of the fact that its content may be embedded on such a child-directed site; and
    c. Clarify that such analytics and advertising networks and content platforms are exempt from COPPA's access and deletion provisions.
5. Replace the current 100% deletion requirement with a **"reasonable measures" standard**, as proposed.

I. Promoting Parental Control & Empowerment

The Congressional architects of COPPA were clear about their goals:

> (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.[3]

This vision is consistent with the general preference for parental empowerment in their children's media consumption over government censorship as expressed in a line of First Amendment cases that began with *ACLU v. Reno* a year before COPPA's enactment. COPPA itself was narrowly tailored to avoid burdening the free speech rights of adults and of websites that speak to them in that it requires verifiable parental consent only when sharing personal information occurs on sites either (i) directed at children under thirteen or (ii) that have actual knowledge they children are sharing personal information. The FTC's decision not to recommend revision of these key provisions4 demonstrates that the agency appreciates the delicate balance struck by COPPA.

COPPA's attempt to "enhance parental involvement" and "parental consent" is also consistent with spirit of the Court's subsequent decisions striking down prescriptive solutions in favor of those emphasizing user choice and empowerment. That philosophy was best by Justice Kennedy's memorably poetic opinion for Court's majority in the 2000 case of *U.S. v. Playboy*:

> The Constitution exists precisely so that opinions and judgments... can be formed, tested, and expressed. What the Constitution says is that these judgments are for the individual to make, not for the Government to decree, even with the mandate or approval of a majority. Technology expands the capacity to choose; and it denies the potential of this revolution if we assume the Government is best positioned to make these choices for us.[5]

No better standard has ever been offered for government to deal with the concerns raised by the digital revolution: Government bears the burden of justifying regulation, and should always begin by advancing empowerment solutions before making choices for us. Just how to apply this vision online is increasingly at the heart of technology policy debates ranging from COPPA to privacy more generally. Specifically, the question facing policymakers today, and judges in the coming years, is: At what point do government efforts to promote user choice in fact

---

[3] 144 Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (statement of Rep. Bryan).

[4] 76 Fed. Reg. 59805, 59806 (Sept 2, 2011).

[5] *U.S. v. Playboy*, 529 U.S. 803, 818 (2000) (striking down a requirement that adults opt-in to having adult cable unscrambled in favor of an opt-out), available at www.law.cornell.edu/supct/html/98-1682.ZO.html

become, despite their liberating intentions, tantamount to government decrees in practice? And when do such efforts actually produce the opposite of what the government intends to decree?

II. General Pitfalls of Empowerment-by-Decree

Whenever government mandates an opt-in regime—like COPPA—it risks over-riding the preferences of users in subtle ways. The Court has begun to grapple with this disconnect: This summer, in *Brown v. EMA*, the Court struck down a California barring the sale of video games to minors, which California "justified in aid of parental authority: By requiring that the purchase of violent video games can be made only by adults, the Act ensures that parents can decide what games are appropriate."[6] The Court disagreed:

> the Act's purported aid to parental authority is vastly overinclusive. Not all of the children who are forbidden to purchase violent video games on their own have parents who care whether they purchase violent video games. While some of the legislation's effect may indeed be in support of what some parents of the restricted children actually want, its entire effect is only in support of what the State thinks parents ought to want.[7]

The Court elaborated on this point:

> … parents have traditionally had the power to control what their children hear and say. This is true enough. And perhaps it follows from this that the state has the power to enforce parental prohibitions—to require, for example, that the promoters of a rock concert exclude those minors whose parents have advised the promoters that their children are forbidden to attend. But ***it does not follow that the state has the power to prevent children from hearing or saying anything without their parents' prior consent***. The latter would mean, for example, that it could be made criminal to admit persons under 18 to a political rally without their parents' prior written consent—even a political rally in support of laws against corporal punishment of children, or laws in favor of greater rights for minors.... Such laws do not enforce parental authority over children's speech and religion; they impose governmental authority, subject only to a parental veto.[8]

A mandatory opt-in is simply the imposition of government authority subject to a veto. We must ask how effective that veto actually is, and to what extent the law effects not in parents' choices, but government's. This is particularly true for any changes the FTC might make to COPPA.

---

6 *Brown v. EMA*, No. 08-1448 (June 27, 2011), at 15, http://www.supremecourt.gov/opinions/10pdf/08-1448.pdf (emphasis added).

7 *Id*. at 16.

8 *Id*. at 7 n 3.

COPPA says a parent must opt-in by providing "verifiable consent" before their child may share information. As in *Brown*, this amounts to a "veto" over the government's decision against such sharing. But the veto is costly, both for operators to offer and for users to exercise. Thus, when government designs a "choice architecture," it does not simply channel parents' preferences into choices, it necessarily re-shapes, and often frustrates them. As I explained in my comments on the FTC's preliminary staff report on Privacy last January, citing the Nobel Prize winning economist Ronald Coase:

> Coase's key insight was that, in a perfectly efficient market, the outcome would not depend upon [whatever rules government might impose]: To put this in terms of the privacy debate, the choice between, say, an opt-out rule and an opt-in rule for the collection or use of a particular kind of data (essentially a property right) would have no consequence because the parties to the transaction (say, website users and website owners) would express their "true" preferences perfectly, effortlessly and costlessly. But, of course, such frictionless nirvanas do not exist.[9]

Betsy Masiello and Nicklas Lundblad have categorized four key ways opt-in can frustrate user choice given the real world costs of time, energy and money required from users and sites:

> **Dual cost structure**: Opt-in is a partially informed decision because users lack experience with the service and value it provides until after opting-in. Potential costs of the opt-in decision loom larger than potential benefits, whereas potential benefits of the opt-out decision loom larger than potential costs.
>
> **Excessive scope**: Under an opt-in regime, the provider has an incentive to exaggerate the scope of what he asks for, while under the opt-out regime the provider has an incentive to allow for feature-by-feature opt-out.
>
> **Desensitisation**: If everyone requires opt-in to use services, users will be desensitised to the choice, resulting in automatic opt-in.
>
> **Balkanisation**: The increase in switching costs presented by opt-in decisions is likely to lead to proliferation of walled gardens.[10]

The current landscape of children's content reveals all four problems. The recent study by Danah Boyd and others examines the problems of desensitization and excessive scope:

> many parents now knowingly allow or assist their children in circumventing age restrictions on general–purpose sites through lying. By creating this environment, COPPA inadvertently hampers the very population it seeks to assist and forces parents and children to forgo COPPA's protection and take greater

---

[9] Berin Szoka, *Written Comments on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"* (2011), http://tch.fm/s2JmX5.

[10] Nicklas Lundblad & Betsy Masiello, *Opt-in Dystopias*, 7 *SCRIPTed* 155 (2010).

> risks in order to get access to the educational and communication sites they want to be part of their online experiences.[11]

The FTC itself probably cannot fix the problems identified by by Boyd and her colleagues. It remains unclear how best to implement COPPA's lofty goals of empowerment For the time being, it might well be that, to paraphrase Churchill on democracy, COPPA is the worst way to deal with children's privacy—except for all the others. A clear alternative has yet to be presented. But any revisions to COPPA should be assessed with these failure modes in mind—and avoid exacerbating these problems.

III. Algorithmic Filtering to Prevent Sharing Personal Information

While commonly understood as a restriction the collection of information for marketing, COPPA's definition of "collection" also requires verifiable parental consent for sharing personal information with other users (on sites covered by COPPA).[12] Among the best aspects of the NPRM is the FTC's proposal to replace the current "100% deletion requirement" with:

> a ''reasonable measures'' standard whereby operators who employ technologies reasonably designed to capture all or virtually all personal information inputted by children should not be deemed to have ''collected'' personal information. This proposed change is intended to encourage the development of systems, either automated, manual, or a combination thereof, to detect and delete all or virtually all personal information that may be submitted by children prior to its public posting.[13]

As I emphasized in my 2009 Senate testimony on COPPA,[14] this change could go a long way to minimizing the burden of COPPA on the expression of children, and interactivity of child-directed sites, by allowing sharing without the burden of obtaining verifiable parental consent. This concept is also very much consistent with Justice Kennedy's vision of technological empowerment—and it mitigates, at least somewhat, the potential First Amendment problem identified by the Court in *Brown*: "it does not follow that the state has the power to prevent children from hearing or saying anything without their parents' prior consent."[15]

---

[11] Danah Boyd et. al., *Why Parents Help their Children Lie to Facebook about Age: Unintended Consequences of the 'Children's Online Privacy Protection Act'*, 16 First Monday, (2011) http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075 ("*Boyd Study*").

[12] 16 C.F.R. § 312.2 (definition of "collects or collection").

[13] NPRM at 59808.

[14] COPPA 2.0 at 19 ("sites could potentially allow children to communicate with each other through chat rooms, message boards, and other social networking tools without having to obtain verifiable parental consent if they had in place algorithmic filters that would automatically detect personal information such as a string of seven or ten digits that seems to correspond to a phone number, a string of eight digits that might correspond to a Social Security number, a street address, a name, or even a personal photo—and prevent children from sharing that information in ways that make the information ''publicly available'').

[15] *Brown v. EMA* at 7 n 3.

IV. The Need for Effective Consent Management Systems

COPPA was conceived under a paradigm of websites as the primary experience of the Internet. But since 1998, the Internet has evolved towards a paradigm of platforms that support applications, whether those apps run on social networking sites like Facebook, mobile operating systems like the Apple iPhone's iOS, Microsoft's Windows Phone, and Google's Android, online gaming systems like Microsoft's XBox Live, or desktop browsers like Google's Chrome. Simultaneously, systems of "federated identity" have emerged from Facebook, Twitter, Google and even Mozilla's Firefox (BrowserID). Together, these application platforms and "federated identity management" systems are enabling an unprecedented abundance and diversity of content, innovation, and competition among a wide range of players, from large to small. But so far, this paradigm is essentially limited to general audience sites.

If we want children under 13 to be able to enjoy such sites *without* simply lying about their age[16]—in other words, if we want meaningful parental control *and* the other values identified above (abundance, innovation, competition, affordability, etc.)—we must ensure that COPPA makes it feasible to build systems of "consent management" that will allow parents to consent not just on a site-by-site basis—a choice architecture in which their "veto" of government decision against sharing is difficult—but across apps and services within a platform that satisfy their preferences. Realizing Justice Kennedy's vision of parental empowerment will require making choice easier, not harder, for parents—effective *across* platforms, not limited to single sites and services.

Any consent management service provider needs to be able to obtain consent on behalf of others without assuming liability for all their actions. Holding the provider legally responsible for any violations of COPPA committed by those using their platform may *sound* privacy-enhancing, but in practice, it will chill, if not entirely prevent, the development of the very mechanisms parents need to be effectively empowered in the the era of web platforms. This is very much akin to the motivation behind Section 230 of the Communications Decency Act of 1996: Congress over-ruled the liability imposed on publishers by the common law for material they published that was created by third parties because deputizing them as intermediaries simply would have prevented the flourishing of platforms for user generated content.[17] Simply put, COPPA should ensure that a service provider may obtain consent on behalf of others without liability so long as it has in place reasonable mechanisms for ensuring compliance.

V. The Pitfalls of Abolishing Email Plus

Ironically, by abolishing email plus, the FTC would make it more difficult parental consent more difficult to obtain online even as the expansion of the definition of "personal information" would subject many more operators to COPPA—especially third party operators of analytics, advertising and embeddable content platforms who have no easy way to obtain parental

[16] *Cf*. *Boyd Study*.

[17] 47 U.S.C. § 230.

consent, as discussed below. Making parental consent more difficult to obtain would disproportionately burden smaller players in the market and retard new entry, especially when combined with the burden placed on the network advertising on which so many smaller publishers depend. This would reduce competition as well as abundance and innovation.

The FTC suggests, as alternatives to email plus, using last four digits of a person's social security number or government-issued identification information.[18] Here, the litigation over COPA is again instructive. The courts emphasized the subjective concerns of Internet users who might be deterred by age verification requirements. The Third Circuit approvingly quoted the district court, which had noted that part of the reason age verification requirements deterred users from accessing restricted content was "because Internet users are concerned about security on the Internet and because Internet users are afraid of fraud and identity theft on the Internet."[19] The district court had held that:

Requiring users to go through an age verification process would lead to a distinct loss of personal privacy. Many people wish to browse and access material privately and anonymously, especially if it is sexually explicit. Web users are especially unlikely to provide a credit card or personal information to gain access to sensitive, personal, controversial, or stigmatized content on the Web. As a result of this desire to remain anonymous, many users who are not willing to access information non-anonymously will be deterred from accessing the desired information.[20]

Relying on even part of social security numbers and government identification might raise similar concerns for many parents—exacerbating the "dual cost" problem. The very general uneasiness about privacy that COPPA is concerned with could become a reason that COPPA frustrates parents' values and judgments if the law requires too many opt-ins by parents—much as the Court held California's ban on violent videogame purchases by minors to frustrate, rather than serve, consumer choice.

Instead, the FTC should promote the development of the technological solutions it considered in the NPRM but declined to adopt, including electronic signatures and the use of parental control systems such as in gaming consoles and mobile devices. Ideally, parents should be able to authorize certain kinds of "collection" by trusted sites through the parental control software on their child's phone, console or other device, or through parental control tools as yet unavailable on social networks like Facebook for children under 13.

Adoption of these tools should not wait another five years for another revision of the COPPA rules. Whatever the FTC ultimately decides about email plus, the FTC could accelerate understanding of alternative consent verification technologies by, for example, holding a workshop dedicated to discussing such technologies, and how, if possible, to facilitate their use without another full-scale rule revision cycle.

---

[18] NPRM at 59818.

[19] *American Civil Liberties Union v. Ashcroft*, 534 F.3d 181, 196 (3d Cir. 2008).

[20] *ACLU v. Gonzales*, 478 F. Supp. 2d 775, 805 (E.D. Pa. 2007).

The FTC should clarify two related questions:

- If a site is required to delete the information it uses to verify the parental relationship, how will it later prove that it properly established the parent child relationship?
- Will the FTC "grandfather-in" consent previously obtained under email plus? The cost, and practical difficulty, of re-obtaining verifiable parental consent for such information could be considerable, especially for small sites.

VI. Problems Raised by Including Persistent Identifiers in "Personal Information"

Just as the web has evolved towards platforms for applications, it has evolved towards networks for analytics and advertising, and platforms for content, especially user generated content, that are integrated across the web. While this results in more data collection, it is not clear that redefining "personal information" to subject such collection to COPPA's verifiable consent requirement will actually serve the values outlined above. In general, defining "personal information" more broadly aggravates the "excessive scope" and "densensitization" problems: The more often parental consent is required, the less meaningful it will be. But a host of other problems are raised by the FTC's two-fold expansion of "personal information" to include:

> (g) A persistent identifier, including but not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier, where such persistent identifier is used for functions other than or in addition to support for the internal operations of the Web site or online service;
>
> (h) an identifier that links the activities of a child across different Web sites or online services;[21]

A. Unintended Consequences of for Network Analytics & Advertising

The NPRM says paragraph (g) "is designed not to interfere with operators' ability to deliver content to children within the ordinary operation of their Web sites or online services," but specifies that "operators such as network advertisers may not claim the collection of persistent identifiers as a technical function under [this] exemption...." Paragraph (h) contains no such exemption for a third party network's use of identifiers across sites for advertising or analytics purposes, even when "internal" (*i.e.*, limited to within the network itself). Thus, parental consent would be required not merely for network analytics and "behavioral advertising" (based on building a profile of a user's likely interests),[22] which has industry already voluntarily agreed on,[23] but would affect the collection of data required for all contextual network

---

[21] NPRM at 59812.

[22] *Id*. 59812 n. 84.

[23] *Guidelines, DMA Corporate Responsibility* Center, http://www.dmaresponsibility.org/Guidelines/

advertising for purposes such as reporting, fraud detection, ad-sequencing, and frequency capping.

Taken together, government would thus be "imposing its authority" heavily against network analytics and advertising services—two essential aspects of site operation for most websites. This would lead to one of the following outcomes:

1. Some child-directed sites might switch to running advertising and analytics on their own. This is likely unfeasible for all but the largest publishers and will certainly raise costs across the board while reducing advertising revenue, and therefore competition, abundance and innovation.
2. Some child-directed sites might simply abandon advertising and analytics. While some sites could perhaps afford to operate without any ad revenue, even most not-for-profit site operators rely on networks analytics to measure use of their site as a way of understanding how to improve it.[24] Again, competition, abundance and innovation would suffer.
3. Child-directed sites that do not currently collect, or allow the sharing of, personal information that want to continue using network analytics and advertising would have to begin requiring users to log-in and obtain verifiable parental consent. Not only will this cost come at the expense of content creation and innovation, it will mean the collection of *more* information and checkpoints across the kids' Internet. It would be ironic if, in the name of privacy protection, we discouraged anonymous use of child-directed sites and aggravated the problem of desensitization.
4. Some operators will simply (i) pull out of the children's market, (ii) decline to enter it or (iii) to expand their offerings, or (iv) consolidate with other operators.

How would any of these outcomes serve the values of a flourishing children's media landscape?

B. Effect on General Audience Platforms & Services

Unfortunately, the expansion of personal information to include persistent identifiers could also affect general audience sites and services in two respects: (i) as sources for content embedded on child-directed sites and (ii) as hosts of user-generated content that itself might be child-directed.

1. Embedded Material & Widgets

The Web's shift from the website paradigm to the platform paradigm also includes increased integration in the "first-party" site visited by a user of content supplied by third party sites—especially user-generated content. This might include embedding a Vimeo or YouTube video in a single blog post or a "widget" or "gadget" across an entire site—say, of a stream of content generated by a site like Twitter or Tumblr. But what happens if such a platform's content is embedded into a site covered by COPPA? Today, the platform operator is not subject to COPPA because, even though it is present on the COPPA-covered site, it is not involved in "collection"

[24] *See, e.g.*, http://trends.builtwith.com/analytics/Google-Analytics.

of personal information covered by COPPA. But if the definition of "personal information" is expanded to include the persistent identifier information regularly used by these third parties for analytics or advertising purposes (such as displaying an ad in an embedded video), these operators will (in most cases) engage "collection" every time their embedded content is displayed. Will they therefore be covered by COPPA?

One might argue they not subject to COPPA's parental consent requirement because their "portion of a site" is not directed at children? But the NPRM implies the opposite by holding that a network advertiser whose ads are served on a site directed at children would be an operator. The FTC should clarify if this is its view and if the embedded material would also have to be directed to children. In either case, how could such platforms obtain verifiable parental consent in the first place?

And how will such a platform know when to require such consent? How can they determine when their content is embedded on sites directed at children? Even the development of effective "consent management platforms" proposed above will not solve this problem, no matter how well they work for child-directed sites. Thus, to avoid liability, such a platform might feel compelled to require *all* users to log-in, before loading the platform's content embedded *anywhere* on the web—and certify that they are over thirteen. This would likely give rise to a First Amendment challenge to COPPA as applied in this context on the same grounds COPA was struck down: depriving adults of the right to access content anonymously, and depriving platforms of the audience of users unwilling to log-in to access such content.[25] But of course, simply age-gating access would not satisfy their obligation if they were held to be an operator of a portion of a site directed to children: they would have to obtain parental consent or simply not serve the content. But, again, how could they know when to do so?

While this option is clearly unworkable, other conceivable options are probably worse:

1. Barring embeds on, or requiring consent (or log-in) before loading embeds on, sites listed on a blacklist of sites deemed "child-directed." To avoid liability under COPPA, this would only work if the FTC itself created the blacklist as part of a safe harbor that would insulate the network from liability for failing to block additional sites. Obviously, such a solution would require Congressional revision to the COPPA statute, and would raise a host of First Amendment and practical concerns. It is probably a terrible idea but deserves mention here if only to illustrate how limited a network's options would be.
2. Creating a version of the platform's embed system that does not load a tracking element or persistent identifier. But since it is publishers and users who would place the embed code on COPPA-covered sites, and absent a blacklist of COPPA-covered sites, there is no way for the network to ensure that the tracking-free version would be used.
3. Simply not loading tracking elements or persistent identifiers into *any* embeds. This would impose a huge cost across the industry, not merely in financial terms (from lost advertising revenue) but in the loss of ability to measure, and further improve, speech

[25] *See COPPA 2.0* at 24-27.

through analytics. It might well be unconstitutional as a restriction on the free speech rights of website operators, another element of the *COPA* decision.[26]

None of these options are feasible. So the FTC has three options—two of them workable:

1. Not include persistent identifiers as, on their own, "personal information"
2. Include an exception in paragraph (h) for the network or platform's internal operations akin to that in paragraph (g) for a site's internal operation—though this might still force some networks to change their practices if they use information collected through their embeds and widgets for broader purposes. This would not be consistent with the essential virtue of COPPA heretofore: that its effect has been limited to child-oriented websites. COPPA was never intended to be a back-door way of regulating the broader Internet.
3. Include such an exception in paragraph (h) *and* specify that content platform shall not be considered an operator subject to COPPA (thus needing recourse to such a definition exception in the first place) solely because content may be embedded on a child-directed site. This would permit network-based analytics and advertising, so long as data was not shared outside a network, while also avoiding the problem detailed immediately above of applying COPPA to platforms whose content is embedded on child-directed sites.

2. Child-Oriented Material on User-Generated Content Sites

What about child-oriented material on platforms such as YouTube? Today, such sites are generally accessible to all visitors without log-in, though log-in is required before using additional features such as commenting (which would clearly qualify as "collection" under COPPA). Like any general audience site, they are not considered to be generally subject to COPPA because they are not "directed at" children. As part of initially configuring an account, users are asked their age and denied access if their answer indicates they are over 13—thus avoiding "collection" in cases where the site has actual knowledge it is "collecting" personal information from users under 13.

While COPPA provides that a *portion* of a site may be deemed "directed at children," just how this provision might be applied in the context of large user-generated content sites remains unclear. Might a single video qualify as directed to children? What about a channel created by a producer geared towards children's content?[27] FTC seems never to have brought an enforcement action based on these distinctions, and the FTC's COPPA FAQ does not address them.[28] But perhaps this question has not been addressed because no "collection," as currently

---

[26] *See COPPA 2.0* at 26.

[27] *See, e.g.*, Vimeo Channel: Kidproof http://vimeo.com/channels/kidproof, YouTube Channel: Nursery Rhymes: HooplaKidz http://www.youtube.com/user/hooplakidz?v=327R1NH5jYg&feature=pyv&ad=18890046568&kw=children#p/a

[28] http://www.ftc.gov/privacy/coppafaqs.shtm

defined by COPPA, occurs on these sites prior to log-in, and log-in at least in theory bars children from creating an account?

But if personal information is expanded to include persistent identifiers, merely visiting such a site to watch a video—or viewing such content embedded outside the platform—would result in "collection" of "personal information." This is not just true for videos but for a wide range of content hosted on platforms that rely on advertising for revenue and analytics to track usage and inform site design and optimization—*i.e.*, most if not all major social networks, from blogs to photo sharing sites, that are currently navigable without log-in. Whatever this FTC might intend today, if a future FTC were to decide that a channel or user page on a social networking service like Facebook or Twitter or Google+ (or even a single piece of content) constituted a "portion of the site" "directed at children," the platform would no longer be able to rely on the assumption that general audience sites are immune from COPPA's burdens—an assumption that has, thus far, distinguished COPPA from the unconstitutionality of COPA. Even if speculative concerns arose that such liability might exist, the future evolution of such platforms might be affected.

At the very least, this concern might lead general audience websites that do not currently age-gate to begin doing so, on the assumption that, if sites that currently collect personal information avoid COPPA by doing so, this procedure would protect sites that currently collect only personal identifiers. The burden of such age-gates on the speech rights of general audience operators and users would raise same free speech concerns as COPA.

COPPA's current carve-out from the definition of "Website or online service directed to children" does not seem to address this issue: "a commercial website or online service, or a portion thereof, shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link." This failure is hardly surprising, given that COPPA was written before the rise of UGC platforms. The FTC could be heading for a minefield of unintended consequences by expanding definition of personal information to mean these platforms are "collecting" information from visitors.

C. Problem with Access and Deletion Rights if "Personal Information" Expands

Access and correction/deletion rights are core principles of the Fair Information Practice Principles (FIPPS). COPPA's general principle that parents have the "right... to review personal information provided by a child" makes sense given the current definition of "personal information." But expanding the definition of personal information to include persistent identifiers leads to a host of problems regarding access rights.

COPPA's access rights are a double-edged sword for privacy. In order to prevent unauthorized access, they require some system for ensuring that the person accessing information about a child is, in fact, their parent.[29] Establishing that relationship with any certainty is the central

[29] COPPA requires that an access system "Ensure that the requestor is a parent of that child, taking into account available technology." 16 C.F.R. § 312.6(a)(3)(i).

weakness of COPPA's real-world implementation. Absent a government-run database that ties parents to children, with all its ominous implications, operators have only crude proxies for verifying this relationship. Thus, in general, the more information is subject to access rights, the larger the problem of potential leakage of information and the greater the tendency will be to increase the collection of information for authentication purposes—not one but two ironic results for a law intended to *protect* privacy. In short, more log-ins will be required to access content that is currently available for children to visit without requiring any "collection."

This problem worsens when dealing with persistent identifiers. If the only personal information a site or network has is a persistent identifier like a cookie or an IP address, will that alone be an adequate basis for authenticating access to logs associated with those identifiers? Would this not mean that anyone using a particular computer or other device could access logs of Internet use conducted from that computer or device? In the case of advertising, analytics and embeddable content platforms, how could such access be limited to logs of visits to (or embed views on) child-directed sites? "On the Internet, nobody knows you're a dog"—and in this case, how could the operator distinguish between the parent, the child and anyone else who might happen to get access to devices, especially mobile devices that are easily accessible outside the home? If an analytics or ad site tracks all use on a device across the Internet and is unable to distinguish between child-directed and general audience sites when it presents log information to whoever happens to be using a computer with the associated cookie or persistent identifier, what would stop a clever child from viewing all of his *parents'* web use? Or what would stop a child from viewing a log of his own Internet use (whether limited to child-directed sites or otherwise) and deleting all or part of the log to hide something from his parents?

Access and deletion rights are probably unworkable for unauthenticated data not tired to a specific individual. The best way to avoid these problems would, of course, leave the definition of personal information as-is—or at least to exempt information used solely for purposes internal to the network. Failing those, the FTC should exempt such information from the access requirement.

Assuming it could be done at all, how could network operators who supply advertising, analytics or content embedded on child-directed among other sites distinguish between data collected on these two categories of sites? If they cannot do so effectively, how could they feasibly implement access rights only for data they collect on child-directed sites? Or would COPPA require access rights more broadly?

Finally, how could raw analytics and advertising log files be presented to parents in a useful fashion that satisfies COPPA's requirement that an access system "not be unduly burdensome to the parent?"[30]

[30] 16 C.F.R. § 312.6(a)(3)(ii).