KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

BEYOND BRIGHT SHINY OBJECTS: SITUATING CHILDREN'S PRIVACY WITHIN A COMPREHENSIVE PRIVACY FRAMEWORK

By Leslie Harris

April 8, 2011

Washington is experiencing a "Privacy Spring": the online privacy debate has been rejuvenated and for the first time in over a decade, privacy is back on the policy table. Both the Federal Trade Commission (FTC) and the Department of Commerce have issued reports setting out robust frameworks for privacy protections,[1] bills are being introduced in Congress,[2] and the Obama Administration has announced support for baseline privacy legislation.[3]

Not surprisingly, teenagers have become a focal point of the current debate over online privacy, tracking, and advertising. Thirteen years ago, concern about online collection of children's personal information led to the enactment of the Children's Online Privacy Protection Act (COPPA). Now, children's advocates and policy makers have a more complex set of concerns: data-sharing by teens on social networking sites, behavioral advertising, data collection by mobile applications, and advertising campaigns aimed at teens that offer prizes and gifts in return for personal data.[4] These concerns have prompted a raft of new

---

[1] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; U. S. Department of Commerce, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (Dec. 2010), *available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf (hereinafter "DOC Green Paper").

[2] H.R. 611, 112th Cong. (2011) (Rep. Bobby Rush's Building Effective Strategies to Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards (BEST PRACTICES) Act); H.R. 654, 112th Cong. (2011) (Rep. Jackie Speier's Do Not Track Me Online Act); Senators John Kerry and John McCain have also announced plans to introduce a baseline bill within the next few weeks.

[3] The State of Online Consumer Privacy: Hearing Before the H. Comm. on Commerce, Sci., and Transp., 112th Cong. (2011) (testimony of Hon. Lawrence Strickling, Assistant Secretary of Commerce for Communications and Information, National Telecommunications and Information Administration, U.S. Dept. of Commerce) (hereinafter "Testimony of Lawrence Strickling").

[4] *See, e.g.*, Comments of Center for Digital Democracy et al., *In re* Implementation of the Children's Online Privacy Protection Rule, Docket No. 339 (Fed. Trade Comm'n. 2010), *available at* http://www.ftc.gov/os/comments/copparulerev2010/547597-00046-54855.pdf (hereinafter "CDD Comments"); Comments of Common Sense Media, *In re* Implementation of the Children's Online Privacy Protection Rule, Docket No. 339 (Fed. Trade Comm'n 2010), *available at* http://www.ftc.gov/os/comments/copparulerev2010/547597-00036-54846.pdf (hereinafter "CSM Comments").

proposals to address the perceived shortcomings of COPPA, including its application only to children under 13. Proposals have ranged from an expansion of the COPPA age to cover older minors under 18,[5] a Do Not Track (DNT) law for kids,[6] and a Fair Information Practices (FIPs) law that addresses the collection and use of teens' data.[7] In this piece, I argue that that the drive for additional child and/or teen specific privacy laws is counterproductive and threatens to divert policy makers from the urgent task of enacting a comprehensive baseline privacy law for all Americans. Concerns about teen privacy will best be addressed through a strong comprehensive privacy law that requires adherence to Fair Information Practices by all commercial entities, including advertisers, that collect and use personal data.

It is important to understand that none of the practical or constitutional barriers to age-specific privacy legislation have diminished in the years since COPPA. COPPA requires operators of websites and online services directed to children to obtain verified parental consent before collecting any contact information from a child under the age of 13. COPPA's coverage only of minors age 12 and under was not an accident. The initial versions of the bill extended coverage to all minors under 18,[8] but civil liberties groups (including CDT), library associations, reproductive health organizations, and youth rights groups advocated strenuously on behalf of older minors' rights to access and post information[9] online without prior parental approval.[10]

COPPA's narrowed scope saved the law in a number of ways. (Indeed, COPPA is the only federal online child safety or privacy law never challenged in the Supreme Court.) In addition to avoiding the obvious First Amendment challenges to restricting older teens' access to information, the law's focus on young children allows the statute to set obligations for sites and services "directed to children," rather than covering the web at large.[11] The distinction between a site directed to children and one aimed at a general audience is relatively easy to make: the FTC will consider the subject mater, age of models, language, and other characteristics of a site to determine whether it is directed to children,[12] including "whether it uses animated characters, or whether advertising appearing on the website is directed to children."[13] COPPA can rely on the reasonable, easily perceivable difference between websites like Club Penguin that clearly target young children and websites that serve the rest of the population. It does not require general websites to proactively determine users' age, and thus avoids the constitutional and

---

[5] CSM Comments, *id.* at 4.

[6] Common Sense Media, Protecting Our Kids' Privacy in a Digital World (December 2010), *available at* http://cdn1.www.commonsensemedia.org/sites/default/files/PRIVACY_WhitePaper_Dec2010_1130_02.pdf.

[7] CDD Comments, *supra* note 5, at 42-43.

[8] S. 2326, 105th Cong. (1998) § 2(1).

[9] COPPA defines "collect" to include permitting a child to make information publicly available, thus covering all user-generated content sites, regardless of whether they solicit contact information from children directly. 16 C.F.R. §312.2 (definition "collects or collection").

[10] *See* S.2326, The Children's Online Privacy Protection Act of 1998, Hearing before the Subcomm. on Commc'n of the S. Comm. on Commerce, Sci. and Transp., 105th Cong. (1998) (testimony of Deirdre Mulligan, Center for Democracy & Technology)

[11] Operators must also obtain verifiable parental consent if they have actual knowledge that a user is under 13. 16 C.F.R. § 312.3.

[12] 16 C.F.R. § 312.2 (definition of "website or online service directed to children").

[13] Federal Trade Commission, Frequently Asked Questions about the Children's Online Privacy Protection Rule, *available at* http://www.ftc.gov/privacy/coppafaqs.shtm.

practical problems with mandatory online age verification.[14] Any effort to move beyond COPPA, whether to impose its parental consent requirements on teens under 18, adopt a DNT scheme for teens, or enact a teen-specific set of Fair Information Practices will have to grapple with these same concerns and more.

The constitutional barriers to imposing limits on teens' access to information have not diminished in the years since COPPA. Minors have strong free speech rights under the First Amendment. The Supreme Court has made clear that "only in relatively narrow and well-defined circumstances may government bar public dissemination of protected material to [minors]."[15] Outside of the context of sexual material that may be deemed "harmful to minors" or "indecent," minors, especially older teens, have a right to receive information just as adults do.[16] Requiring parental consent or placing specific age-based restrictions on the collection of teens' data may limit their access to information. If the history of COPPA is a guide, it is most likely that sites, when faced with the cost and the legal risk posed by teen specific restrictions will simply revise their terms of service to indicate that their sites are intended for users over the age of 18 or stop hosting " teen-friendly" content.

In the years since COPPA was enacted, the dream (for some) of an age-verified Internet has been shattered. Age verification technologies simply do not work and pose a host of additional constitutional concerns. This was the conclusion, hard-won over almost a decade of litigation, in the cases that overturned the Child Online Protection Act, which aimed to restrict minors' access to indecent material online.[17] That line of cases also established that age verification mandates violate adults' rights to access information anonymously, by requiring them to provide personal information (age/date of birth or credit card information) prior to accessing a website; minors' rights to access information, because many sites simply bar minors rather than face liability due to imperfect age verification; and website operators' rights to reach their audience, because of

[14] That said, there are some significant drawbacks to the COPPA approach. Innovation has foundered under the weight of COPPA's parental consent requirement, leading to an online environment where the few sites tailored to children are locked behind a pay wall, because the simplest method of obtaining COPPA-compliant "consent" is to charge an adult's credit card. And the COPPA model's reliance on consent is somewhat outdated. As the complexity of data collection and uses practices grows, it becomes increasingly clear that an indication of user "consent" cannot be treated like a blanket authorization for companies to collect and use data in any way they seem fit. Because it is rarely possible for a company to explain in a concise and clear manner how it will use data it collects, it is unwise to assume that parents who consent to data collection on behalf of their child have a deep understanding what types of data are being collected and how that data will be used.

[15] Erznoznik v. City of Jacksonville, 422 U.S. 212-13 (1975).

[16] *See* Board of Education v. Pico, 457 U.S. 853, 867-68 (1982).

[17] ACLU v. Gonzales, 478 F. Supp. 2d 775 (E.D. Pa. 2007), *aff'd*, ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008) (finding that age verification services do not "actually reliably establish or verify the age of Internet users. Nor is there evidence of such services or products that can effectively prevent access to Web pages by a minor. . . . Credit cards, debit accounts, adult access codes, and adult personal identification numbers do not in fact verify age." *Id.* at 800, 811); *see also* Internet Safety and Technical Task Force, Child Safety & Online Technologies 28-31 (Dec. 2008), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf ("Age verification and identity authentication technologies are appealing in concept but *challenged in terms of effectiveness*. Any system that relies on remote verification of information has potential for inaccuracies." *Id.* at 10); *see also* Berin Szoka & Adam Thierer, COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech (June 2009).

the prohibitive costs of age verification systems and the chilling effect that requests for personal information have on users' willingness to access information.[18]

A Do Not Track (DNT) mandate for teens raises a fresh set of concerns. DNT technologies that give consumers greater control over behavioral tracking offer great promise but are still in their infancy.[19] Browser makers are currently testing different technical approaches,[20] standards bodies are just beginning to look at DNT,[21] and there is still no agreement on a definition for the term.[22] What does it mean not to "track"? Does it mean no collection and correlation of data even by first party sites? Or is it limited to tracking, collecting and linking personal data across sites? There are also sharp differences of opinion as to whether Congress should enact a DNT mandate, and questions about what the effect of doing so now will have on innovation in DNT implementations. One need look no further that the V-Chip to see the risks to innovation that come with prescriptive technical mandates.[23]

The proposal by a diverse set of child advocacy, public health, and consumer groups including the Center for Digital Democracy, the American Academy of Pediatrics, and Campaign for a Commercial Free Childhood for a teen-specific set of Fair Information Practices consistent with the OECD guidelines comes closest to a sensible proposal, insofar as it abandons the failed notice-and-consent regime in favor of a full set of substantive Fair Information Practices.[24] But it too fails to fully grapple with the age verification conundrum and the likelihood that, when faced with more complicated procedures for teen users' data alone, sites will simply disavow their teen

---

[18] *See, e.g.*, Mukasey, 534 F. 3d at 197 (discussing the difference between online age verification systems and offline restrictions on minors access to harmful-to-minors material that "do not require adults to pay for speech that would otherwise be accessible for free [and] do not require adults to relinquish their anonymity to access protected speech . . . .").

[19] CDT first proposed the idea of Do Not Track as a privacy-enhancing technology that might improve online privacy in 2007. Consumer Rights and Protections in the Behavioral Advertising Sector (Oct. 2007), http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf.

[20] Jordan Robertson, "Microsoft Unveils 'Do Not Track' IE Feature" (Dec. 7, 2010), Associated Press, *available at*

http://www.msnbc.msn.com/id/40554324/ns/technology_and_science-security/; Julia Angwin, Web Tool On Firefox To Deter Tracking, Wall St. J., January 24, 2011, *available at* http://online.wsj.com/article/SB10001424052748704213404576100441609997236.html.

[21] Microsoft, Web Tracking Protection: W3C Member Submission (Feb. 24, 2011), http://datatracker.ietf.org/doc/draft-mayer-do-not-track/; http://www.w3.org/Submission/2011/SUBM-web-tracking-protection-20110224/; W3C, Team Comment on the "Web Tracking Protection" Submission, http://www.w3.org/Submission/2011/01/Comment/.

[22] Press Release, Center for Democracy & Technology, CDT Releases Draft Definition of 'Do Not Track', Jan. 31, 2011 available at http://cdt.org/pr_statement/cdt-releases-draft-definition-do-not-track.

[23] *See, e.g.*, Brief of Amici Curiae Center for Democracy & Technology and Adam Thierer, Senior Fellow With the Progress & Freedom Found, CBS Corp. et al. v. FCC, No. 06-3575 (3rd Cir. Nov. 29, 2006), *available at* http://www.cdt.org/speech/20061129circuit3.pdf; Brief of Amici Curiae Center for Democracy & Technology and Adam Thierer, Senior Fellow with the Progress & Freedom Found., FOX Television Stations, Inc. v. FCC, No. 06-1760-ag (L) (2nd Cir. Nov. 29, 2006) *available at* http://www.cdt.org/speech/20061129circuit2.pdf.

[24] CDD Comments, *supra* note 4, at 42-43.

users. The proposal seems better suited for a best practices discussion with advertisers than for a legislative mandate.[25]

The real question that policymakers need to ask when faced with demands for teen-specific privacy laws is whether it makes sense to provide privacy protections for the 17-year-old and leave the 18-year–old – and, for that matter, the 40-year-old and everyone else – with little or no privacy protection. Compared to its peers, the United States provides very little privacy protection for consumer data.[26] Now, for the first time in many years, there is momentum toward enactment of a baseline law. Consumer awareness and concern over issues like behavioral advertising and web tracking is at an all-time high.[27] The Department of Commerce is promoting its co-regulatory framework while the White House is pushing for enactment of a "privacy bill of rights" and encouraging expanded FTC enforcement authority.[28] Legislation has been introduced in the House and a bi-partisan bill is expected in the Senate.[29] A consensus on the structure of a bill is emerging: broad coverage of both online and offline data practices, adherence to a robust set of Fair Information Practices, a modern definition of personal information which recognizes the diminishing distinction between PII and non- PII, heightened protections for sensitive information, strong enforcement by both the FTC and state Attorneys General and an FTC-supervised safe harbor program to tailor the Fair Information Practices mandate to specific industry sectors that collect and use personal information.[30] The Department of Commerce Report has gone further and proposed that industry specific safe harbor "codes" should be developed through multi-stakeholder convenings that would give privacy and children's advocates, among others, a seat at the table.[31] That proposal will likely be reflected in a bi-partisan bill that will be introduced in the Senate shortly.[32]

The children's advocacy community needs make a choice: Continue to advocate for unworkable age-specific laws or get behind the effort to enact a strong baseline law, raise the level of

---

[25] In the years since COPPA, there have been few specific best practices guidelines developed by industry that relate to teens. The only exceptions are the ratings systems developed by the video game and movie industries. In my discussions with industry, it is clear that concerns about such self-regulatory programs becoming "a stalking horse for regulation" have stymied progress. While those concerns are not unjustified – both the video game and movie industries have repeatedly fought efforts to legislate their ratings systems; in video games' case, this fight has gone all the way to the Supreme Court – self-regulatory measures should not, in my view, be taken off the table.

[26] For example, the U.S. and Turkey are the only two members of the OECD that do not have a baseline consumer privacy law.

[27] What They Know, Introduction Page, Wall St. J., http://blogs.wsj.com/wtk/ (last visited

Feb. 17, 2011).

[28] Jennifer Valention-Devries and Emily Steel, White House to Push Privacy Bill, Wall St. J., Mar. 16, 2011, http://online.wsj.com/article/SB10001424052748704662604576202971768984598.html; Testimony of Lawrence Strickling, *supra* note 4.

[29] BEST PRACTICES Act, *supra* note 3; Julia Angwin, Proposed Bill Would Put Curbs on Data Gathering, Wall St. J., Mar. 10, 2011, http://online.wsj.com/article/SB10001424052748704629104576190911145462284.html.

[30] BEST PRACTICES Act, *supra* note 3; DOC Green Paper, *supra* note 2; Ira S. Rubinstein, Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes, I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY (forthcoming Winter 2011), 22-23 available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275.

[31] DOC Green Paper, *supra* note 2.

[32] Angwin, Proposed Bill Would Put Curbs on Data Gathering, *supra* note 29.

privacy protection in the United States for everyone, and play a role in making sure that industry specific codes address their concerns. Given Congress's tendency to gravitate to bright shiny objects, there is a risk that, rather than grapple with the complex issues posed by comprehensive privacy legislation, the 112th Congress could chose the a teen DNT mandate or other unworkable but easy-to–campaign-on measure aimed only at teens. And that would be a shame for everyone's privacy.