Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

In the Matter of	**)**	
	)	
A Preliminary FTC Staff Report on Protecting	**)**	**File No. P095416**
Consumer Privacy in an Era of Rapid Change	**)**	

COMMENTS OF COMMON SENSE MEDIA

For more than 40 years, using a variety of tools, "the Commission's goal in the privacy arena has remained constant: to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits of the ever changing marketplace."[i]

However, a recent survey conducted for Common Sense Media by Zogby International highlights ways that people are growing *less* confident about the online marketplace:

- 85 percent of parents say they are more concerned about online privacy than they were five years ago.
- 75 percent of parents don't think social networking sites do a good job of protecting children's online privacy.
- 91 percent of parents think search engines and social networking sites should not be able to share kids' physical location with other companies until parents give authorization.
- 93 percent of adults – and 81 percent of teens – said they would take more time to read terms and conditions for websites if they were shorter and written in clear language.
- 88 percent of parents – and 85 percent of teens – want online companies to get their *opt in* before the companies use their personal information for marketing.[ii]

These survey results illustrate how the current problems with protecting personal information in a rapidly changing digital world may also pose longer-term challenges to the growth of online commerce and engagement. As in the "offline" world, users want a marketplace that is safe and reliable. When users feel that an environment is not trustworthy, they will be reluctant to participate. This was also shown in research conducted by the Federal Communications Commission for the development of the National Broadband Plan, which found that:

> 22 percent of non-adopters [of broadband] cite factors pointing to lack of digital literacy as the main reason they are not online. These include people who are not comfortable with computers or, for non-Internet users, are "worried about all the bad things that can happen if I use the Internet."[iii]

As the Federal Trade Commission report documents, many companies today – both online and offline – are not doing an adequate job of protecting personal information and building trust with users. This is especially true for children and teens, who are early adopters of online and mobile technology and who will likely engage in digital marketplaces even more extensively as they become adults.

The proposed framework outlined in the Preliminary FTC Staff Report outlines important principles for improving protections for online privacy. Common Sense Media's comments will address each of these principles and highlight key areas where additional measures should be taken, especially for kids and teens, who need more protections for their personal information, and better preparation for the time when they will be independent adult consumers.

Principle 1: Privacy by Design

Privacy by Design is extremely important and addresses a core challenge in the world of technology. Online and digital media environments change rapidly, and engineers and designers are constantly striving to innovate and to find new ways to connect users. These innovations can bring great value for users, but we have seen many cases where the drive for more and better connections can lead to gaps in protections.

Industry leaders need to embrace the principle that privacy concerns should be addressed in the earliest stages of innovation and built into the resulting designs. Privacy officers within technology companies need to be included throughout the design process, rather than brought in to apologize after a privacy breach.

For some time, Common Sense Media and other advocates have been calling for industry leaders to apply their innovation skills to the challenges of protecting personal information. As we wrote in our recent policy brief, *Protecting Our Kids' Privacy in a Digital World*, "innovation in the online industry over the past decade has been truly amazing; the industry should apply that same spirit of innovation to creating solutions."[iv]

Since the FTC called for a Do Not Track mechanism in this report, it has been encouraging to see industry leaders like Firefox[v], Google[vi], and Microsoft[vii] introducing new tools that will help users block unwanted tracking. It remains to be seen whether these opt-out mechanisms will be honored by the online advertising and marketing industries, but they are positive first steps and signs of what can happen when companies take the lead and innovate to protect privacy.

- The FTC should continue to push for these innovations, especially for kids and teens.
- As importantly, the FTC should push advertising and marketing companies to respect the preferences expressed by users through these new opt-out mechanisms.

Principle 2: Simplified Choice

Simplified Choice is an essential step to improving protections for privacy and personal information in the digital world. Companies and operators need to simplify processes so that users understand what personal information they are agreeing to provide in exchange for a service, why the information is needed, and how it will be used.

Some industry advocates have complained that this would require users to opt in each time they use email or a social network, but this is a red herring. Users should get a simple mechanism to make an informed choice when they *first* use a site or service and, subsequently, when the site or service makes a *substantial* change in its privacy policies or practices, such as when a company or operator decides that it will begin sharing users' personal information with third parties.

As importantly, these opportunities must involve *informed* choice. A user must understand what he or she is agreeing to in order for the agreement to be valid, especially when the user is a child or teen. The report noted this distinction when highlighting that

> both sensitive information and sensitive users may require additional protection through enhanced consent. The Commission staff has supported affirmative express consent where companies collect sensitive information for online behavioral advertising and continues to believe that certain types of sensitive information warrant special protection, such as information about children, financial and medical information, and precise geolocation data.[viii]

Information about children is *fundamentally* sensitive and warrants special protections, including a stronger requirement of affirmative express consent from parents *before* children's movements on the Internet or other personal information is collected or used. Teens are also sensitive users, and companies should be required to get affirmative express consent from older teens *before* collecting or using their information.

There are many steps to strengthening privacy protections, but one of the most important and effective would be for the industry to change the standard on choice from "opt out" to "opt in."

- The FTC should push industry leaders to make these changes, and if they will not, then policymakers may need to take action.

Privacy by Design + Simplified Choice = Do Not Track Kids

Another crucial step to strengthening privacy, which involves both Privacy by Design and Simplified Choice, is the principle of Do Not Track Kids – i.e., companies should not collect and use kids' personal information in order to market or advertise to them.

As a nation, we have long recognized that children are not ready to make the same kinds of decisions that adults are. There are many ways in which we establish protections for kids, including in the financial arena – where for example, they cannot get credit cards without parental consent. It is widely recognized that children, especially at younger ages, cannot really distinguish between content and advertising. That is why Congress established limits decades

ago on TV advertisers targeting kids. We need similar rules in the online world, where the line between content and advertising is even more blurred.

Tracking of private, personal information – potentially including geolocation information – for behavioral marketing and advertising purposes is neither safe nor sensible when applied to kids. We would not allow companies to track every step a kid takes in the offline world, and we shouldn't allow it online, either. In fact, some types of behavioral marketing to children – because of the lack of informed consent from children or parents – seem to clearly fit the definition of unfair and deceptive trade practices.

There are a variety of terms and definitions used to describe behavioral marketing, targeted advertising, and other forms of tracking.[ix] Some companies use different terms, or argue that their approach to advertising or marketing isn't tracking. However, if a company, operation, platform, or third-party application collects personal information and uses it to serve specific advertising or marketing to a user, common sense says that's behavioral advertising, targeted marketing, and tracking.

Not all tracking is necessarily negative. As outlined in our privacy policy brief, some forms of online tracking are functional and helpful, such as:

- Site-specific cookies that make a website experience smoother;
- Signing up for email newsletters or sports updates; and
- Use of location-based applications.[x]

Websites and online companies can use limited tracking to provide a better online experience. But when these tools are used to market to kids, they're not helping anyone but marketers, and kids need to be treated differently than adults.

The FTC report also asked whether these choice principles should be "extended beyond online behavioral advertising and include, for example, behavioral advertising for mobile applications." Clearly, for children, they should. Children today do not *go* online. They *live* online, and they live there through social networks, mobile devices, videogame players, and many other platforms. The distinctions between platforms are no longer meaningful. We need protections for children – and tools for parents – that work across all platforms in the mobile, digital space.

Principle 3: Greater Transparency

This principle is the lowest-hanging fruit in the proposed framework. Privacy policies should be easy for users to find and understand, but for many users today, they are not. For example, in the Common Sense/Zogby survey, 83 percent of parents said "no" when asked whether they "had ever agreed to let an online site collect your child's personal information so that your child could use the website or service."[xi] In addition, as Commissioner Rosch noted in his concurring statement, some companies' privacy policies have been "buried, incomplete, or otherwise ineffective."[xii]

As importantly, even when privacy policies are not hard to find, they are difficult to read, especially for kids and teens who obviously are nowhere near ready for law school. A quick review of the length of privacy policies of five popular websites provides one illustration:

Google: 1,651 words
Facebook: 5,860 words
Yahoo: 1,451 words
YouTube: 1,429 words
Amazon: 2,884 words[xiii]

Lawyers for companies and operators will insist that privacy policies are lengthy because they must address detailed laws and regulations, and that is a fair point. But since the goal is informed consent and the audience is not primarily lawyers, a great deal could be accomplished by summarizing privacy policies and possibly by adding icons or using standardized grids of information so that users can more easily find the information they want when making their decisions.[xiv]

- The FTC should set a standard for policy summaries and push companies to take other steps to make their policies more transparent.

The FTC Report proposal that companies should provide reasonable access to data collected about users is also important, but it's only a first step. Users also need tools to maintain some control over their personal data that has already been collected. One great example would be an Eraser Button: a tool that users – especially parents and kids – could use to delete information they have provided about themselves. While there is no way to erase *everything*, and users must take responsibility and kids must learn to act responsibly, the industry could help by providing better tools.

Another crucial step toward greater transparency is a broad effort by all stakeholders to educate users about data privacy – not only about a company's privacy practices, but about ways that users can take steps to protect their own, and their family's, information.

Industry leaders should make serious commitments to public awareness campaigns, provide clearer and more accessible information on their sites, and support digital literacy and citizenship education. These steps will better prepare users to manage their personal information online, especially the kids and teens who will be the consumers of tomorrow. All technology companies can help with this public awareness and education, but companies that already provide technology and information literacy programs – such as Internet Service Providers and tech device manufacturers – are especially well positioned to help more people learn how to protect their privacy and personal information online.

Conclusion

Policymakers must establish baseline principles for privacy so that industry leaders have targets for their innovations. As we have seen, the best innovations in this space will come from industry. As we have also seen, some companies have been slow to innovate unless pushed by policymakers and principles.

Without clear baseline principles for privacy – and without industry respect for principles that have already been established in laws such as the Children's Online Privacy Protection Act – we will continue the ongoing "arms race" between advertisers and ad-blocking technologies, constantly trying to catch up with ever-changing technologies and never making complete progress. Consumer trust in the online marketplace will continue to suffer – especially among the children who will be the next generation of consumers. And the efforts of the best companies will be undermined by those of the worst, damaging all of their reputations, and hurting the long-term commercial success of the digital marketplace.

---

[i] "Protecting Consumer Privacy in an Era of Rapid Change" Executive Summary

[ii] Common Sense Media / Zogby International survey, August 2010. Summary available at www.commonsensemedia.org/privacy. Complete survey results attached as Appendix.

[iii] "Broadband Adoption and Use in America" OBI Working Paper Series No. 1, by John Horrigan, Ph.D., Federal Communications Commission, February 2010.

[iv] "Protecting Our Kids' Privacy in a Digital World," Common Sense Media, December 2010. Available at www.commonsense.org/privacy and attached as Appendix.

[v] http://blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/

[vi] https://chrome.google.com/webstore/detail/hhnjdplhmcnkiecampfdgfjilccfpfoe

[vii] http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx

[viii] "Protecting Consumer Privacy in an Era of Rapid Change," Preliminary FTC Staff Report, page 61.

[ix] For example, the Interactive Advertising Bureau says that "Behavioral targeting uses information collected on an individual's Web browsing behavior such as the pages they have visited or the searches they have made to select which advertisements to be displayed to that individual." www.iab.net/media/file/GlossaryofInteractivAdvertisingTerms.pdf

[x] "Protecting Our Kids' Privacy in a Digital World," Common Sense Media, December 2010. Page 3.

[xi] Common Sense Media / Zogby International survey (Appendix) question 8.

[xii] "Protecting Consumer Privacy in an Era of Rapid Change," Preliminary FTC Staff Report, page E-2.

[xiii] Word counts of online policies on Feb 8, 2011. As we know, policies are subject to change.

[xiv] For example, in "Standardizing Privacy Notices: An Online Study of the Nutritional Label Approach" researchers at Carnegie Mellon University found that "standardized privacy policy presentations can have significant positive effects on accuracy of information finding, overall speed, and reader enjoyment with privacy policies." http://www.cylab.cmu.edu/research/techreports/2009/tr-cylab09014.html