


Protecting Our Kids' Privacy in a Digital World

A Common Sense Policy Brief

December 2010 / Common Sense Media

Common Sense Media

650 Townsend Street
San Francisco, CA 94103

 415.863.0600

 www.commonsense.org

www.facebook.com/commonsensemedia

www.twitter.com/commonsensenews

Common Sense Media is dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive in a world of media and technology.

Go to www.commonsense.org for thousands of reviews and expert advice.

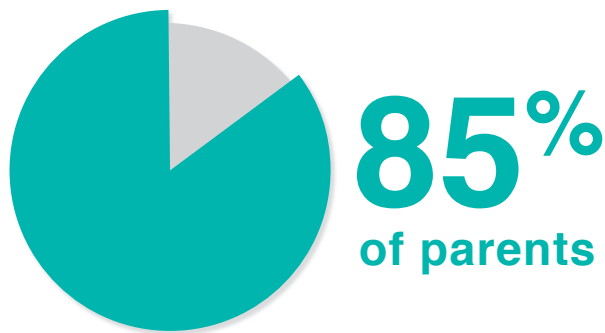
Most kids today live their lives online, immersed in a mobile and digital landscape. This brave new world has revolutionized childhood. Kids and teens now create and consume enormous amounts of online and mobile content. Their access to people and information presents both possibilities and problems. While the Internet is a platform for innovation and economic growth and brings rich resources for entertainment and learning, the very nature of digital interaction creates deep concerns about kids' privacy.

Today, our kids are growing up in public. Whatever they text or post can be searched, copied, pasted, distributed, collected, and viewed by vast invisible audiences. Parents rightly fear that their children's activities and personal information are being tracked and traced.

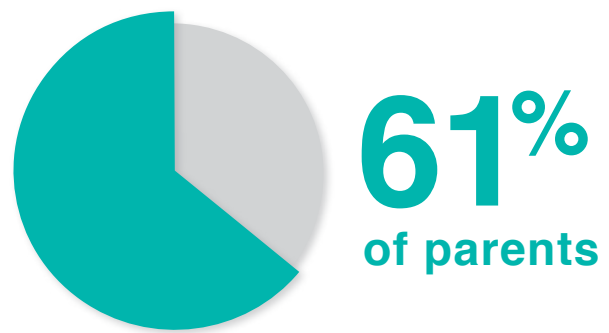
Tracking and profiling children online has quickly become a widespread practice. *The Wall Street Journal* recently found that 4,123 cookies and other pieces of tracking technology were installed on a test computer that was used to visit the top 50 websites for children and teens – 30% more than a *Journal* test of the top 50 overall sites, which are generally aimed at adults.

So what privacy protections do our children have – and what protections should they have? At the moment, there's mainly a law written in 1998, when Google was just beginning and Facebook and Zynga didn't exist. The Children's Online Privacy Protection Act (COPPA) prohibits the collection of "personally identifiable" information – including name, phone number, email or street address, and Social Security number – from children ages 12 and under without parental consent. COPPA remains the cornerstone policy protecting children's online privacy, but the technological advances that have occurred since 1998 make COPPA woefully out of date for keeping children safe from new threats to their privacy.

This brief lays out principles for a new public policy agenda to protect the privacy of children and teens online.



say they are more concerned about online privacy than they were five years ago. *Common Sense/Zogby Survey, 2010*



say Congress should update laws related to online privacy and security for children and teens. *CSM*

principle 1

Do Not Track Kids

Children and teens should not have their online behavior tracked or any other personal information about them profiled by third parties or transferred to third parties. The 1998 COPPA categories of “personally identifiable” information (e.g. name and address) must be updated to include other “persistent identifiers” and to encompass all of kids’ online activities. What children and teens do online should remain private.

Companies – whether Internet service providers, social networking sites, third party application (“app”) providers, data-mining companies, or advertising networks – should not be permitted to sell or transfer that personal information.

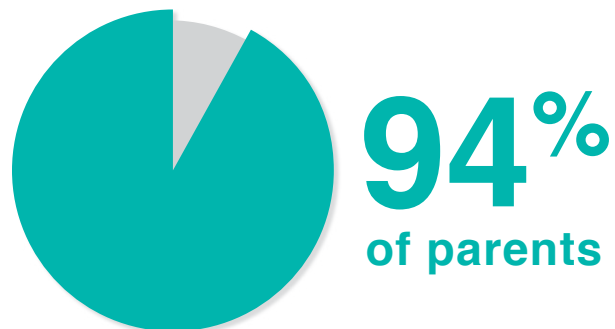
principle 2

The Eraser Button – Parents and Kids Should Be Able to Delete Online Information

Children and teenagers should have the opportunity to delete information they have provided about themselves. Too often we hear about young people who post information they later regret and find they can never fully delete from the online world. Children post personal information on websites, virtual worlds, social networking sites, and many other platforms. Children also make mistakes.

Web companies should develop tools that make it easier for young people – or their parents – to completely opt out and delete this information. Technological 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 like an “eraser button” so that no 15-year-old has to live the rest of his or her life with the consequences of a poor decision about what to post online.

This is the very least we should expect from a technology industry that has repeatedly created new ways to challenge accepted norms of privacy and human behavior. Their ingenuity and resources can certainly build eraser buttons that maximize the ability to erase personal information.



(and 92% of teens) say they should be able to request the deletion of all their personal information held by a search engine, social network, or marketing company after a specific time period. CSM

No Behavioral Marketing to Kids

Today many companies troll the Internet to collect our kids' detailed information in order to target them with "behavioral marketing" – advertising that is specifically tailored to their age, gender, interests, and activities. Behavioral marketing to kids is unfair and deceptive, and it should stop now.

Without parents or kids knowing it, companies collect, store, and sell information about what kids do online and on mobile phones. Companies can install "cookies" or other devices that track which websites kids visit, including which pages they look at; what searches they make; which videos they download; who they "friend" on social networking sites; what they write in emails, comments, or instant messages; and more. And thanks to new "geo-location services," companies can now also track where kids go in the physical world as well as the virtual one.

In addition, kids should not be made into marketers themselves through "viral marketing" strategies. Many sites aimed at kids now promote their content by offering kids access to special games or rewards if they email a web link to their friends – who are then invited to visit the site. It's hard enough for parents to protect their own kids' privacy without also having to worry about other kids sharing friends-of-friends information in exchange for online rewards.

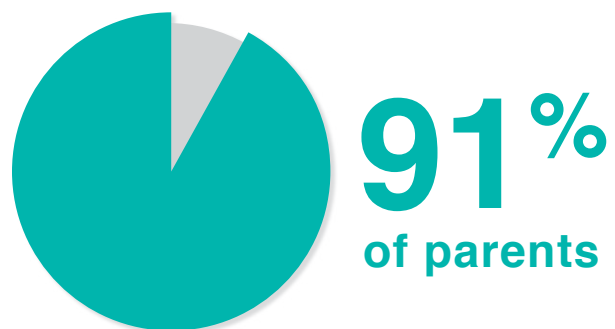
Some online tracking is a helpful aspect of Web 2.0 technology, and parents or teens should be able to "opt in" to limited use of tracking devices, as long as they are not used for behavioral marketing and are not transferred to third parties. For example:

Site-specific cookies that are designed to offer users a smoother experience on the website, such as remembering a password for future site visits, pausing a game online, or remembering what's in a user's shopping cart.

Sharing their email address if they want to receive newsletters, sports scores, or other notifications from a website. However, Web operators should use the email address only for the specific purpose the kid signed up for – not transfer it to a third party or use it for behavioral marketing.

Use of location-based applications.

Companies should continue to be able to provide location-based applications to children with parental permission and to teenagers who opt in. However, location-based information about children and teens should not be stored, transferred, combined with other data, or used for behavioral marketing.



(and 81% of teens) say search engines and social networking sites should not share their physical location with other companies without their specific authorization. CSM

principle 4

The Industry Standard for All Privacy Should Be Opt In – Especially for Kids

Companies and operators must make significant changes in the ways that they collect and use kids' personal information. Most importantly, the industry standard should be "opt in" – in other words, companies and operators should not collect or use personal information unless users give explicit prior approval.

The opt-in standard is fundamental to our ability to control our personal information. If online companies, services, and applications want to collect and use personal information, they should get permission beforehand by asking people to opt in to the service.

Too many online companies launch new services – such as location-based applications – and enroll users automatically, giving them the opportunity to opt out afterward. This can mean that a kid's personal information is collected and used before the kid or the parents even understand how the service works. All online companies, services, and third-party application providers should follow an industry standard of getting an opt in, especially for kids.

principle 5

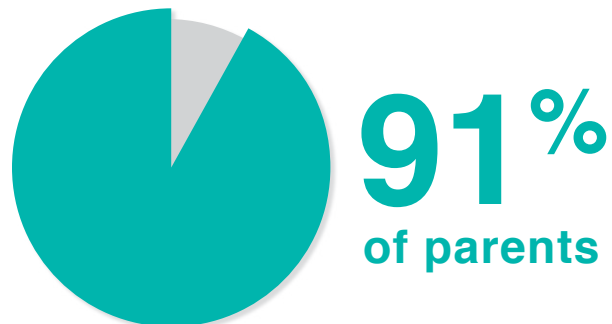
Privacy Policies Should Be Clear and Transparent

Privacy policies need to be easy for users to find and understand and should be carefully monitored and enforced. Any significant privacy policy changes should require a clear new opt in by the user – or the parent, depending on the age of the child.

We all want instant access to online content and are often too quick to click the "I accept" box to get where we want to go. For young children and teenagers, the impatience and temptations are probably even greater, and the risks posed to their privacy may seem further removed.

Most privacy policies today are lengthy legal documents written at a college level or beyond. Instead, companies should use icons and symbols that would be easy to understand and would clearly convey how users' personal information will be used.

In addition, some sites have one privacy policy for the site itself and other policies that apply if users click on an application or advertisement, resulting in complex layers of legalese that are virtually



(and 81% of teens) say they would take more time to read terms and conditions for websites if they were shorter and written in clear language. CSM

impossible to follow. We need clear, succinct language for privacy policies. We also need third-party ratings of privacy policies so that parents and kids can get independent information about how policies work.

Online providers should also be held accountable for monitoring and enforcing their privacy policies. Far too many breaches of websites' privacy policies have been allowed to occur. For example, a *Wall Street Journal* investigation revealed that many Facebook applications – including the 10 most popular ones – sent users' unique Facebook IDs to outside advertising or data mining companies, even if the user's Facebook account had been set to "private." According to Facebook, this was a violation of the site's own rules. Companies that build their business on people sharing personal information need to ensure that they can fully protect that information and enforce their own policies.

principle 6

Parents and Children Should Be Educated About Online Privacy

Kids and their parents need to do their part to protect their online privacy – and the privacy of their friends. We need a large-scale, multi-year public education campaign to help them learn how to do so effectively, and it should be funded by industry.

While this brief outlines steps that industry and policymakers should take to protect children's privacy online, it is also important that families take responsibility for protecting their privacy themselves. Young people need to learn to protect their own privacy and to respect others' privacy.

The online/mobile world is changing so rapidly that children, teachers, and parents all need to be educated about online privacy. There should be a digital literacy curriculum in every school in this country, with privacy as an essential component of that curriculum.

principle 7

Privacy Protections Should Apply Across All Online and Mobile Platforms

Many kids today don't go online – they always are online, whether from their home computer, cell phone, or Web-connected video game player. For the same reason, current privacy regulations need to be clarified and applied to all online and mobile services and platforms. Social networking sites shouldn't be able to collect or sell kids' private information, and neither should third-party apps on those sites. Location-based services shouldn't be allowed without prior consent, regardless of whether the service is provided by a non-FCC carrier.

Conclusion

As a nation, we need to protect the privacy of children and teenagers in the mobile and online worlds in which they live by building on several key principles:

1. Do Not Track Kids

2. The Eraser Button: Parents and Kids Should Be Able to Delete Online Information:

Easy-to-use “eraser buttons” will let parents or teens fully delete information they no longer want online.

3. No Behavioral Marketing to Kids: Children and teens should not be targeted using their online personal information.

4. The Industry Standard for All Privacy Should Be Opt In – Especially for Kids

5. Privacy Policies Should Be Clear and Transparent: Privacy policies need to be easy for users to find and understand and should be carefully monitored and enforced.

6. Parents and Children Should Be Educated About Online Privacy: A major new privacy education program will help parents and kids do a better job of protecting their own and others’ privacy.

7. Privacy Protections Should Apply Across All Online and Mobile Platforms: Privacy protections should apply to all platforms – including laptops, cell phones, and Web-connected video game consoles – and to all providers, including apps, ad networks, and websites.

Children’s online privacy addresses two key American concepts: our fundamental right to privacy and our need to protect our children from potential harm. The extraordinary technological changes and new mobile and social media platforms that have developed in recent years have created entirely new environments for children and teens, with unprecedented implications for their privacy. It is time to update our nation’s privacy policies for the 21st century. Everyone needs to be a part of this new effort: industry, families, schools, policymakers, and young people themselves. Public policy can and should lead the way to common sense solutions.

WHO WE ARE

Common Sense Media is dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive in a world of media and technology.

More than 1.6 million people visit the Common Sense website every month for age-appropriate media reviews and parenting advice. Tens of millions more access our advice and information through our distribution partnerships with leading companies like Comcast, DIRECTV, Verizon, Time Warner Cable, Cox Communications, Facebook, Yahoo!, Google, Apple, Disney, Netflix, Best Buy, AOL, Symantec, and more.

COMMON SENSE MEDIA BOARD OF DIRECTORS

Rich Barton	Co-Founder and Exec. Chair, Zillow.com	Robert L. Miller	President and CEO, Miller Publishing Group
Marcy Carsey	Founding Partner, Carsey-Werner Productions	William S. Price, III (Chair)	President, Classic Wines, LLC
Chelsea Clinton	New York University	Jesse Rogers	Founder, Altamont Capital
James Coulter	Founding Partner, TPG	Susan F. Sachs	Interim President and COO, Common Sense Media
Geoffrey Cowan	University Professor, The Annenberg School for Communication at USC	James P. Steyer	Founder and CEO, Common Sense Media
April McClain-Delaney	President, Delaney Family Fund	Gene Sykes	Managing Director, Goldman, Sachs & Co.
John H.N. Fisher	Managing Director, Draper Fisher Jurvetson	Todor Tashev	Director, Omidyar Network
Lycia Carmody Fried	Community Volunteer	Deborah Taylor Tate	Former FCC Commissioner
Thomas J. Holland	Partner, Bain & Company, Inc.	Michael Tollin	Founding Partner, Tollin Productions
Mitchell Kapor	Director, Mitchell Kapor Foundation	Lawrence Wilkinson (Vice Chair)	Co-Founder, Oxygen Media and Global Business Network
Gary E. Knell	President and CEO, Sesame Workshop	Anne Zehren	CEO, Kaboodle.com

BOARD OF ADVISORS

Aileen Adams	Chair, The Women's Foundation of California	David Lawrence Jr.	President, The Early Childhood Initiative Foundation
Larry Baer	President, San Francisco Giants	Nion McEvoy	Chairman and CEO, Chronicle Books
Richard Beattie	Chairman, Simpson Thacher & Bartlett LLP	Nell Minow	Founder, The Corporate Library and Movie Mom
Angela Glover Blackwell	Founder and CEO, PolicyLink	Newton Minow	Counsel, Sidley, Austin and Brown; Former FCC Chairman
Geoffrey Canada	Founder and President, Harlem Children's Zone	James Montoya	Senior Vice President, The College Board
Ramon Cortines	Superintendent, Los Angeles Unified School District	Becky Morgan	President, Morgan Family Foundation
Yogen Dalal	Managing Director, The Mayfield Fund	Nancy Peretsman	Managing Director, Allen & Company Inc.
Steve Denning	Founding Partner, General Atlantic Partners	Philip Pizzo, MD	Dean, Stanford University School of Medicine
Susan Ford Dorsey	President, Sand Hill Foundation	George Roberts	Founding Partner, Kohlberg Kravis Roberts & Co.
Millard Drexler	Chairman and CEO, J. Crew	Carrie Schwab Pomerantz	President, Charles Schwab Foundation
Ezekiel Emanuel, MD, PhD	Chair, Department of Clinical Bioethics, The National Institutes of Health	Alan Schwartz	CEO, Guggenheim Partners
Robert Fisher	Director, GAP Inc.	Marshall Smith	Senior Adviser, Department of Education
Arjun Gupta	Founder & Managing Partner of TeleSoft Partners	Thomas Steyer	Founding Partner, Farallon Capital
F. Warren Hellman	Founding Partner, Hellman & Friedman	Robert S. Townsend	Partner, Morrison & Foerster LLP
James Herbert II	President and CEO, First Republic Bank	Laura Walker	President, WNYC Radio
David Hornik	Partner, August Capital	Eugene Washington, MD	Dean, UCLA Medical School
Omar Khan	President, Insight Strategy & Logic (ISL), Web Site Design	Alice Waters	Founder, Chez Panisse and Chez Panisse Foundation
		Robert Wehling	Founder, Family Friendly Programming Forum; Former CMO, Procter & Gamble
		Tim Zagat	Co-Founder and Co-Chair, Zagat Survey