Inside the Kids' Privacy Zone

What Parents and Policymakers Need to Know to Keep Kids Safe and Smart Online

common sense kids action®

Introduction

With the explosive growth of digital devices and "smart" toys, education technology in the classroom, and social and mobile media, today's youth are living their lives almost entirely online at home, at school, and on the go. New high-tech tools offer wonderful potential for our kids to learn, communicate, and create, as well as the potential for others to amass personally identifiable information about young people that can be tracked, mined, and exploited by unintended audiences with unexpected consequences over the course of a lifetime. Today's kids need to learn how to be safe and smart online to thrive in the modern world. And parents and policymakers, as well as industry and educational leaders, all have an important responsibility to help our kids succeed.

Failure to address privacy protections for young people, coupled with concerns about increasing corporate and government surveillance, poses several serious threats for our society and economy. First, children and families risk losing control over their basic privacy and their right to autonomy. Young people may temper their exploration and self-censor their thoughts or withhold information, whether online or when in homes with smart speakers or among friends with smart glasses. Second, the personal and financial security of children and families is at risk. With increasing concerns over identity theft, hacks, and data breaches, it can be hard for families to feel their children are secure. Ultimately, failure to address these threats could undermine our collective trust in technology. Young people need opportunities to engage with technology in ways that don't put their physical or financial safety at undue risk. And they need the freedom to make mistakes, try new things, and find their voices, unencumbered by the looming threat of a permanent digital record that could label them or limit their access to information and opportunities.

As adults, we owe kids this freedom. The landscape has changed, and keeps changing, dramatically and we all need to pay attention, for our kids. As the technology evolves — from the advent of social media to edtech to the Internet of Things — protecting kids' privacy and safety is a continuing concern for parents and should be a concern for policymakers.[1] Parents, in particular, can feel overwhelmed by so many developments in this area.

For over a decade, Common Sense has helped kids, families, educators, businesses, and policymakers navigate the rapidly changing technology world, including protecting kids' privacy. Since we started, technology has morphed, moving from family television screens and clunky laptops to tiny screens and sensors embedded in our clothes and toys. Privacy became a major focus for Common Sense in 2010, when mobile technology was beginning its meteoric rise among young people. We launched a privacy campaign and released a policy brief, **Protecting Our Kids' Privacy in a Digital World**, in an effort to drive a new public policy agenda to protect the privacy of kids and teens online. Today, technology continues to change, but the principles and best practices that drive us — do not track, opt in, access, corporate responsibility, and family engagement — remain the same.

Common Sense is committed to educating parents and policymakers about finding the proper balance in today's rapidly changing media and technology world and to protecting our kids' privacy while enabling them to connect and create. This report examines five pressing privacy developments — smart toys and smart homes, virtual and augmented reality, digital citizenship, targeted ads, and edtech — in the hope that, together, families, schools, policymakers, and industry can lead the way to commonsense solutions to protect our kids.

Common Sense's highly trusted resources for parents and policymakers — covering privacy, cyberbullying, tech addiction, digital citizenship, smart devices, social media, marketing to kids, and much more — are available at **www.commonsense.org**.

[1] E.g., *National poll: Three out of four parents say social networks aren't protecting kids' online privacy.* San Francisco, CA: Common Sense Media (2010). Ninety percent of adults are concerned about how private companies with non-educational interests can access and use students' personal information; *Student privacy survey.* San Francisco, CA: Common Sense Media (2014). Seventy-six percent of adults are concerned about the privacy and security of smart toys; *Our increasingly connected lives.* ESET and the National Cyber Security Alliance (NCSA). (2016).

Background

In 2010, when Common Sense released **Protecting Our Kids' Privacy in a Digital World**, mobile technology and smartphones were beginning their meteoric rise. Since then, the tech world has been busy and so have we: We've advocated for strengthening the Children's Online Privacy Protection Act (COPPA), launched a School Privacy Zone, spearheaded and supported landmark student and youth privacy and digital citizenship legislation in California and across the country[2], and encouraged state and federal updates to better protect our kids and students.[3] We have been the voice for kids' and students' privacy in U.S. Department of Commerce roundtables regarding facial recognition and consumer privacy; with the White House; in the FCC's broadband privacy proceeding; in legislative and regulatory efforts to protect geolocation privacy and Internet of Things privacy; and in protecting Californians' electronic communications privacy. We've worked with companies to encourage best practices and industry leadership on kids' privacy. And in collaboration with school districts across the country, Common Sense developed a first-of-its-kind privacy evaluation tool of popular edtech products.

While specific technology may change, our guiding concepts and animating principles remain the same: Kids and teens should not be tracked and targeted, and they should have control over their personal information. Companies should compete on privacy and build it into their products and services from the ground up. We need better privacy and security protections across platforms, whether those are websites, smartphones, or smart teddy bears. And we all need to better educate ourselves about online privacy and digital literacy.

Parents deserve to know about the constant efforts to collect and mine their kid's information. This isn't all nefarious. In many instances, kid's information is collected to create a more effective learning tool or provide high-quality content at a low cost. But data collection and analysis is happening, and it's not always done with the best interests of our kids in mind. Similarly, policymakers have a responsibility to help establish strong baseline protections for our children and teens, who are particularly vulnerable. These protections can provide rules of the road and certainty for companies and peace of mind for families. And these special protections for youth have long been supported in public policy.

KNOW THE LINGO

COPPA: Why do you need to be 13? Explaining the Children's Online Privacy Protection Act.

COPPA is one of the nation's very few consumer privacy laws. COPPA is designed to give parents control over what personal information websites and apps collect from their young children. That said, COPPA does not prevent companies from collecting information from children or targeting them with ads. Rather, it requires that certain companies get verifiable parental consent before collecting, using, or disclosing children's personal information. COPPA only applies to websites and online services, including mobile apps, that are directed at children under 13 or that are for general audiences but who have actual knowledge that they collect, use, or disclose personal information from children under 13. (This is why many popular sites require users to be 13.) Whether a site is directed at children under 13 involves multifaceted questions about, for example, site subject matter and visual content and whether it would appeal to children, the site's intended audience, the site's actual audience, and what sorts of ads run on the site. "Personal information" generally means information that permits the physical or online contacting of a child. This includes a child's first and last name, geolocation, Social Security number, contact information, photo, video, or voice. It also includes persistent identifiers that can be used to recognize a child over time across different sites. In addition, COPPA requires privacy policies and reasonable security and gives parents certain access and deletion rights.

[2] E.g., Student Online Privacy Information Protection Act (SOPIPA), Early Learning Privacy Information Protection Act (ELPIPA), Eraser Button Act, Delaware Online Privacy and Protection Act.

[3] E.g., Do Not Track Kids Act, Student Digital Privacy and Parental Rights Act, SAFE Kids Act, updates to FERPA

Our Privacy Principles

Common Sense seeks to provide all young people with access to high-quality digital experiences that will help them create, communicate, and learn in new and effective ways while protecting them and their personal information. Our work is grounded in the following principles and practices:

Do not track

Children and teens shall not be tracked online and shall not be profiled or subject to behavioral ads based on their personal information or online activity.

Opt in

Children's and teens' personal information shall not be shared without their parents' or their express, informed consent.

Access

Children and teens shall be able to easily access, modify, and delete the personal information they choose to share.

Corporate responsibility

Companies shall be transparent with families about their privacy and security practices, minimize personal information collection and retention, and appropriately safeguard any personal information they do collect.

Family engagement

Parents and families should educate themselves about their privacy options and the best ways to safely and responsibly create, communicate, and learn online.

KNOW THE LINGO

What Is Privacy by Design?

Privacy by design is the idea that companies should build in privacy and security from the ground up by incorporating sound privacy and security policies and practices at every stage of product development. By incorporating privacy and security into the architecture of a product and involving designers and engineers, along with attorneys and business and policy experts, from the beginning, companies are in a better position to protect consumers and their market share.

As with any important endeavor — raising our kids or enacting public policy — knowing your principles is key to getting the job done right. These principles are intended to help grown-ups, no matter their job, do the right thing for kids.

Privacy in Practice

Five Developments That Parents and Policymakers Need to Understand

The privacy landscape facing kids and families is constantly evolving. By examining some of the challenges and opportunities young people face today, we hope to help parents and policymakers develop commonsense solutions that work for families and for our nation.

1 | Smart Toys and Smart Homes: The Internet of Things (IoT)

These days, everything is — or can be — connected. The "Internet of Things" generally refers to devices and objects, which used to be offline — like toasters, fridges, or teddy bears — but which are now connected to the internet or to each other. This connectivity can enable useful and innovative features such as voice-activated channel surfing, toys that remember a child's name, exercise bands that track your heart rate, or the ability to watch your house's security camera while vacationing. For individuals with disabilities, IoT can be a game changer, such as voice activation for people with limited mobility. IoT also brings security and privacy concerns for everyone. These devices collect sensitive information — such as voice, video, health, and location information — and they are often in traditionally personal, private locations, such as in the home or on one's body. Many of these devices are used by kids, whether they are designed for them or not. The devices share information with each other and with the network, allowing for tracking of individuals not only on one device but across devices. This can allow for more customization and personalization; it also means companies can build a richer profile of a user. Often, this information collection and sharing happens without a user's — or a user's parents' — knowledge or understanding.

Moreover, personal information collected by these devices is often poorly protected. With many device makers focused on developing the latest hit gadget, privacy and security are often an afterthought. Many of these devices are cheap or not able to receive security updates, and devices at all price points are routinely hacked. For example, a hack of the interactive stuffed animals made by CloudPets compromised the personal information of over half a million users, and a cyberattack on toy company VTech exposed the data of 6.4 million kids.[4]

Exposed personal information can leave families vulnerable to identity theft or the ransoming of personal information.[5] It also can create physical security risks, either because a device itself is insecure (allowing someone to find your child's location or to turn off your car remotely) or because it is connected to your home network and can be used as an entry point to take down your smart security or other systems. Indeed, major networks have been taken down by insecure video cameras and DVRs.[6]

KEY PRINCIPLES Opt in, access, corporate responsibility

★ TIPS FOR PARENTS Know before you buy. Try to figure out what information a device will collect, how you will know when it is collecting any sensitive information (by, for example, recording), and how you can turn this function on and off before you bring anything into your home or give it to your kids.

Consider what security upgrades and updates are offered and how to get them, by looking at product packaging or on a product's website.

Change passwords to something stronger than the default.

[4] Gibbs, S. (2015, November 30). Toy firm VTech hack exposes private data of parents and children. *The Guardian;* Hern, A. (2017, February 28). CloudPets stuffed toys leak details of half a million users. *The Guardian.*

[5] BBC News. (2017, March 14). Cyber security: Experts warn on rise of hacker ransoms. Experts predict a rise in the use of ransomware on devices, where hackers make devices -- holding photos, emails, fitness information, or other information -- unusable until owners agree to pay.

[6] Perlroth, N. (2016, October 21). Hackers used new weapons to disrupt major websites across U.S. *The New York Times.*

★ **TIPS FOR POLICYMAKERS** Recognize that many makers of cheap IoT devices have little marketplace incentive to embrace security and privacy but that this can imperil the larger networks and jeopardize family privacy and security.

Encourage transparency both at the point of sale and when consumers are using devices to minimize surprise and give consumers control.

2 | Targeted Advertising and Personalized Content

It's not only that new pair of shoes or a cheap airline ticket following you around the web. Advertising has become ever more dynamic, and these days advertising can be based on any number of things: offline habits and hangouts, age, physical characteristics, family income, shows watched and stories read, shops visited — basically, an individual's entire life. Large data brokers, tech companies, and ad networks seamlessly deliver "personalized" content to us at just the right moment, whether that's on a phone or TV, on a "smart" billboard you walk by that happens to catch your face (and identify it, or just categorize it based on age, ethnicity, or gender), or via a mailer to your teenage daughter with special pregnancy-related offers.[7] Sometimes these ads are woven into native content, virtually indistinguishable to young (or old) eyes. And it's not just ads. One teen's news feed may look very different from her friend's. One child's search query for a school project could lead to different results from his classmates in a wealthier ZIP code across town. One teen's search for summer jobs could lead to different opportunities from another teen's depending on their online histories.

The increasingly personalized and persuasive capabilities of companies raises a number of questions about who controls a child or teen's information, shared unknowingly as they go about their day. It also raises questions about commercialization and commodification of behavior online, with young kids themselves being turned into unwitting marketers, as they participate in viral memes and other activities that may appear user-driven but are actually company-directed. Better safeguards are needed. Knowing that young people are more susceptible to ads — and that the very young cannot distinguish them from other content — it may never be appropriate to target them with ads based on their behavior or certain background characteristics such as race, health, or family income.[8] Ads and personalized content directed at children and teens need particularly clear and obvious disclosures that a young person can understand. Unfortunately, in many cases today, children and teens lack understanding, and they lack control, aside from attempting to self-censor or mask their activities. Moreover, they have little choice. Sites and services typically offer take-it-or-leave-it options presented in privacy policies far too difficult for young people to understand and far too long for anyone to read. Transparency at all levels is lacking.

KEY PRINCIPLES Do not track, opt in, access

★ **TIPS FOR PARENTS** Take advantage of any options to limit targeted ads and data collection on sites and services that you use, and encourage your children and teens to share no more than is necessary.

Help your kids think critically when they are presented with advertising content online and off.

★ **TIPS FOR POLICYMAKERS** Children and teens are uniquely vulnerable to targeted ads, and they should be able to be themselves and be free online without fear of profiling or targeting.

(CONTINUED ON PAGE 7)

[7] Duhigg, C. (2012, February 16). How companies learn your secrets. *The New York Times*.

[8] Peterson, A., & Marte, J. (2016, May 11). Google to ban payday loan advertisements. *The Washington Post*. Some companies have taken aim at stopping predatory advertisements. Google agreed to stop hosting ads for payday lenders, which often exploit the financial desperation of low-income workers, and Facebook agreed to stop allowing advertisers of housing, employment, and credit offers to target viewers by ethnicity; Mahewshwari, S., & Isaac, M. (2016, November 11). Facebook will stop some ads from targeting users by race. *The New York Times*.

(CONTINUED FROM PAGE 6) Children and teens need extra help in identifying advertising content.

If they've shared information online, children and teens should be able to delete it.

3 | EdTech

School is another place where kids are increasingly coming into contact with technology. "Edtech" refers to apps, services, and devices that schools integrate in the classroom and rely on for a variety of academic and administrative functions. Online platforms and websites, mobile applications, digital courseware, and cloud-computing programs track students' attendance and grades, monitor students' physical activity and locations, manage school lunch programs, and offer individualized learning platforms. Schools and edtech providers collect massive amounts of sensitive data about students, including contact information, performance records, online searches, family finances and backgrounds, health information, behavior and disciplinary records, meal selections, and locations. Under outdated laws designed for paper records and file cabinets, schools can share sensitive information about their students. Companies can use this sensitive information to target ads. And this and more sensitive student information is often left exposed by human error or poorly designed security features.[9] All this information can be used by bad actors in unexpected ways.[10]

The use of technology to enhance education and learning holds enormous promise. It also raises concerns that students may be inadvertently exposing themselves to targeted ads, profiling, cross-device tracking, or other unintended consequences of simply trying to get an education. The school zone should be a privacy zone, where students can learn and take advantage of new technology without fear that their information will be used for non-educational purposes.

KEY PRINCIPLES Do not track, corporate responsibility, family engagement

★ **TIPS FOR PARENTS** Ask your schools about what edtech they use, who vets it, and how you can learn more.

Find out what your rights are with regard to the sharing of directory information.

★ **TIPS FOR POLICYMAKERS** Update outdated privacy laws to reflect modern technology.

Edtech companies that collect student information are often the ones in the best position to protect and safeguard students and their information.

4 | Digital Citizens and Digital Footprints

Young people use technology for intimate conversations with friends, everyday chats with parents, and educational and professional interactions with teachers and employers. They set up profiles of themselves and share and create images, videos, and thoughts that can spread farther and last longer than ever before. Tweens are spending over two hours a day with mobile media and almost as much time on screens, watching videos, playing games, using social media, browsing websites, video-chatting, and creating.[11] And teens are spending even more time. This can have long-term consequences, as schools, employers, and other decision makers are

[9] Sanchez, M. (2015, May 19). Data breach triggers sharing of personal info for 4,000 students. *The Chicago Reporter*. Edtech breaches of sensitive student information continue to proliferate. For example, in 2015, Chicago Public Schools accidentally shared the personal information, including disability status, of 4,000 students with five vendors seeking to do business with the district; Ravipati, S. (2017, April 21). Schoolzilla security issue exposes data for 1.3 million students and staff. *The Journal*. In 2017, 1.3 million kids' and staff members' personal information, including standardized test results and Social Security numbers, was compromised in a breach of data warehouse platform Schoolzilla.

[10] Harold, B. (2014, January 22). Danger posed by student-data breaches prompts action. *Education Week*. Reports have even surfaced of mobile dentists targeting lower-income youth for unnecessary procedures, based on student records shared by schools.

[11] Common Sense Media. *The Common Sense census: Media use by tweens and teens*. (2015). San Francisco, CA: Common Sense Media.

paying attention to all of this digital information. Imagine, for example, a teenager who is frequently home late (her timestamp logged by the "smart" home-monitoring system), who is friends with a popular crowd on social media, and who shares posts about parties with pictures of beer cans. She's categorized as an alcohol user and "socially influenced" (even though she doesn't drink), a piece of information seized upon by future employers and school admissions officers. Indeed, not only do college admissions officers often look at applicants' social media accounts, 60 percent of employers report checking job candidates' social media accounts.[12] Even politicians aren't immune to this type of surveillance: One Congressional candidate's college activities were used as fodder for attack ads against him.[13]

These profiling concerns are real, and the results can last a lifetime. Young people may be afraid to fully explore and interact with the world around them and could lose trust in technology, raising concerns about free expression and potentially squelching opportunities for youth to engage with new ideas and audiences. Digital interactions also can have more immediate day-to-day consequences that change behavior, because the other people paying attention to kids and teens online are their friends and classmates. Cyberbullying and sexting are of deep concern to parents. Tech addiction is a growing problem: Fifty-nine percent of adults think their teens are addicted to smartphones, and 50 percent of teens agree they are. Moreover, a third of parents and teens report fighting over smartphone use on a daily basis.[14] To succeed today and in the future, young people need help in learning digital citizenship: how to safely, ethically, responsibly, and effectively use media and technology resources.

KEY PRINCIPLES Opt in, access, family engagement

★ **TIPS FOR PARENTS** Model behavior you'd like your kids to adopt, and institute a device-free dinner or even a device-free car ride.

Understand that good online behavior mimics good offline behavior and that there is no differentiating between the two when it comes to safety, responsibility, and respect.

★ **TIPS FOR POLICYMAKERS** Digital citizenship and media-literacy training are vital to educating, empowering, and engaging kids with the best practices around consuming and producing media.

Support schools in developing a digital citizenship curriculum and professional development around technology, involving educators, administrators, researchers, and parents in developing best practices and resources.

Engage stakeholders in a discussion around clear rules of the road about data minimization: Discuss what information actually needs to be collected and how long it needs to be retained.

5 | Virtual and Augmented Reality: Pokémon Go and Its Progeny

Augmented reality (AR) and virtual reality (VR) are the next frontier of kids' education and entertainment. Augmented reality games and tools overlay computer images onto images of the real world — like the Pokémon who can appear in your yard or the Snapchat sunglasses that appear on your face. Virtual reality, which is less widely adopted, takes this one step further by creating an immersive three-dimensional space that people can interact with like in the real world.

[12] IvyWise. *Social media presence and admissions.* (2012). Number of employers using social media to screen candidates has increased 500 percent over the last decade. (2016, April 28). *CareerBuilder.*

[13] Taylor, J. (2017, March 2). Attack ad marks new era for millennials running for office. NPR.

[14] Common Sense Media. *Dealing with devices: The parent-teen dynamic.* (2016). San Francisco, CA: Common Sense Media.

These games and apps merge the online and offline worlds, creating fun new ways for kids to connect with their friends. They also raise some unique concerns, as we saw with the augmented reality app Pokémon Go. Many apps require location tracking to function, as well as access to a device's camera or other information. They may analyze facial expressions and even emotions. Players are in some ways inviting the games to follow them around all day, collecting information without limit, and opening themselves up to highly specific targeted ads that may be woven into gameplay (for example, you might get extra points for going into the fast-food joint down the street). There are additional physical safety concerns as well. Gameplay can lure individuals to unsafe locations.[15] And because these games and experiences are so engaging, they can distract users, who are often wandering around in a real-world environment. This was a major issue with Pokémon Go, as people — young and old — distractedly risked life and limb, walking into busy intersections, ditches, and lakes, all in pursuit of gaming glory.[16]

Further, another real/virtual line these games often blur is the cost. Many apps appear to be free, but kids and families still pay — either with personal information or through hidden monetary costs in the form of upgraded features, tokens, or capabilities. It can be hard for children or young teens to understand the line between virtual tokens and real cash.[17]

KEY PRINCIPLES Do not track, corporate responsibility, family engagement

★ **TIPS FOR PARENTS** Get to know the games your kids and teens are playing, and talk to them about the importance of paying attention to their surroundings and turning off the apps when they are not in use. Try it together at home with a new app.

Make sure you have your app store settings set to prevent unwanted purchases by your kids.

Set limits on how much time your kids can spend on these games.

★ **TIPS FOR POLICYMAKERS** Parents and teens deserve clear information about costs and capabilities, meaningful choices with respect to sensitive information collection and sharing, and the ability to provide informed consent.

Physical safety concerns must be addressed with mobile virtual and augmented reality games.

Summary

Rapid changes in media and technology offer tremendous opportunity as well as significant challenges. We all must pay greater attention to the privacy and security implications of technology with regard to kids. Parents and teachers must talk to their kids and students, explore the technology, and educate themselves. Industry leaders must find innovative ways to protect kids and privacy. And, while there's much that can be done at home, at school, and by companies, policymakers also are responsible for ensuring that kids' privacy is protected. Common Sense remains committed to ensuring that kids and families have the tools they need so young people can take full advantage of technology to develop their voices, opinions, identities, and communities in a safe, smart, and privacy-protective way.

Common Sense's highly trusted resources for parents and policymakers — covering privacy, cyberbullying, tech addiction, digital citizenship, smart devices, social media, marketing to kids, and much more — are available at **www.commonsense.org**.

[15] Morse, D., & Shapiro, T. R. (2016, July 13). Robbers target Pokémon Go players in Maryland and beyond. *The Washington Post*.

[16] E.g, Tsukayama, H. (2016, July 10). Pokemon Go's unexpected side effect: injuries. *The Washington Post*.

[17] E.g., Federal Trade Commission. (2016, April 27). Federal court finds Amazon liable for billing parents for children's unauthorized in-app charges. The FTC has settled with the makers of Apple, Google Play, and Amazon over unfairly confusing consumers with "free" apps that had in-app purchases available to kids.

CREDITS

Author

Ariel Fox Johnson

Design

Marjerrie Masicat

Copy Editing

Jenny Pritchett

Special Acknowledgement

Danny Weiss and Kelsey Kober

Inside the Kids' Privacy Zone
© 2017 Common Sense Kids Action

SAN FRANCISCO HEADQUARTERS
650 Townsend Street, Suite 435
San Francisco, CA 94103
(415) 863-0600

WASHINGTON, D.C. OFFICE
2200 Pennsylvania Avenue NW
4th Floor East
Washington, D.C. 20037
(202) 350-9992

NEW YORK OFFICE
575 Madison Avenue
New York, NY 10022
(212) 315-2138

LOS ANGELES OFFICE
1100 Glendon Avenue, 17th Floor
Los Angeles, CA 90024
(310) 689-7535

For more resources, visit
www.commonsense.org/kidsaction

common sense kids action®