



Prepared Statement of:

Amy Guggenheim Shenkan

President and Chief Operating Officer

Common Sense Media

United States Senate

Senate Commerce, Science, and Transportation Committee

Consumer Protection, Product Safety, and Insurance Subcommittee hearing:

Consumer Privacy and Protection in the Mobile Marketplace

May 19, 2011

“Protecting Privacy – Especially for Kids – in a Mobile and Digital World”

Good morning, Mr. Chairman, and members of the Committee, and thank you for this opportunity to discuss the crucial issue of protecting consumer privacy in the mobile marketplace.

Common Sense Media is a non-profit, non-partisan organization 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.

Nearly two million people visit the Common Sense website every month for reviews and parent tips about media content and the digital media world. Tens of millions more access our advice and information through our distribution partnerships with leading companies like Comcast, DIRECTV, Time Warner Cable, Cox Communications, Facebook, Yahoo!, Google, Apple, Disney, Netflix, Best Buy, and more.

Common Sense Media commends the Chairman and the Committee for this timely hearing on consumer privacy. The stakes couldn't be higher for all of us, and especially for our nation's kids.

Today, millions of kids don't just go online, they seem to live their lives online. Children and teens today are growing up in a media environment that provides an ever-present and ever-changing experience in a new digital landscape – an environment that is changing childhood. A recent study by Consumer Reports estimated that 7.5 million kids under age 13 are lying about their age to be on Facebook – and that 5 million of those kids are age 10 and under. There are tens of millions more who are 13 through 17.

And kids don't just access content online, they create it. They don't simply interact with their peers online, but with adults and companies too.

And in contrast to the childhoods we all had, today's children are growing up in public. They post, search, copy, “friend,” “un-friend,” tweet, create, distribute, and connect through social networks, apps, and other digital services in ways that can be seen by millions around the world

and gleaned by companies as well, including – but not limited to – the companies represented here today.

The Internet is a worldwide platform for accessing information and realizing new educational opportunities, possessing resources for both entertainment and learning. Yet, with all of the wondrous things that the Internet brings to children and teens, the interaction that such kids have with digital technology, apps, and services raises significant concerns about kids' privacy.

Overall concern about consumer privacy is clearly growing. In a Common Sense Media/Zogby International poll last fall, 85% of parents said they are more concerned about online privacy than they were five years ago.

Moreover, privacy is a concern expressed not only by parents – but by kids too. The same poll found that 91% of parents (and 81% of teens) say search engines and social networking sites should not share their physical location with other companies without their specific authorization.

Yet, lest you think that Common Sense Media is a Luddite organization, let me emphasize that we embrace technological change and innovation and the manifold benefits the Internet and digital media bring to children and teens. One of our founding beliefs is that “we love media.” Like the millions of parents and teachers who come to Common Sense for information, we want to find the best things that the digital media world offers for kids – and there are many

great things – but also want to avoid the things that may not be appropriate for them, especially at younger ages.

We simply believe that a far better balance can and must be struck. A balance that makes available the rich resources of the Internet – but that also protects children and teens from privacy invasions and inappropriate targeted marketing and behavioral advertising. There is no such balance today, and the basic well-being of our children and teens is at risk as a result.

We believe that balance is being struck in a bipartisan way on the House side by legislation introduced by Rep. Ed Markey (D-MA) and Rep. Joe Barton (R-TX), the first major kids’ privacy legislation introduced since 13 years ago – when the founder of Facebook was in grade school.

And as much as we embrace overarching, comprehensive privacy protections for consumers – and especially kids – for all Internet technologies and services, it is clear that the ability to track the mobile whereabouts and habits of an individual as she or he moves throughout our society raises hyper-sensitive privacy issues. Privacy is an issue everywhere in the online world, but in the mobile world, privacy is an issue on steroids. And this nation must address the issue of mobile privacy now. We cannot overstate the urgency of this moment.

For kids, this is absolutely critical – knowing what a child or teen does online at home is one thing. Knowing where they go after school, with whom they visit, what they search for, and what hours they spend where around town is not only incredibly invasive, it is potentially very

dangerous and a fundamental violation of their personal privacy and self-interest. Mobile companies and app developers that have a cavalier attitude about this topic need a very clear wake-up call. While all adults should have “opt-in” protections for location information for all mobile services and apps, it is vitally important to move immediately to protect children and teens in the mobile environment.

Concerns about mobile technology and geolocation have been reinforced in several recent surveys and studies. For example:

- In a survey by Truste, an industry-based organization, 77% of smartphone users said that they don't want to share their location with app owners and developers.
- In a recent Nielsen survey of mobile subscribers who downloaded an application within the previous 30 days, more than half (59% of women and 52% of men) said they are concerned about their privacy when using geolocation services and check-in apps.
- A new study by the Future of Privacy Forum analyzed the top 30 paid mobile apps across the leading operating systems (iOS, Android, & Blackberry) and found that 22 of them – nearly three-quarters – lacked even a basic privacy policy. This is outrageous, especially because kids are such huge users!

It is obvious to most of us and clearly to most parents that our existing protections for privacy and personal information online are grossly inadequate and in no way keeping pace with the rapid changes of our digital and mobile media world.

Congress must address this critical issue for kids and families now. Congress enacted legislation in the late 1990s addressing wireless location information from wireless carriers requiring such companies to obtain the “prior express authorization” of the subscriber for using location information for commercial purposes. But this outdated law did not cover 3rd party services and apps – only wireless companies – and did not contain specific protections for children and teens. That should be changed now.

Moreover, in the case of children, as you know, the Children’s Online Privacy Protection Act (COPPA) is the landmark legislation in this area, but the technological advances that have occurred since 1998 make COPPA woefully out of date for keeping children safe from these vast new threats to their privacy. 1998 is like the medieval ages of digital tech development, but that is when the last privacy law protecting kids was written.

Common Sense Media believes it is way past time to update that Act and to provide major new privacy protections for children and teens, on mobile platforms and elsewhere.

If we want to strike the proper balance, and ensure that America’s kids and adults can realize the benefits, and avoid the potential pitfalls, of the digital world, all of us – parents, educators, policymakers, and industry leaders – can and must take steps to improve protections for our privacy and personal information online, and especially for kids. But Congress must lead now.

For kids, Common Sense Media believes those steps should build on a few basic principles. The first is Do Not Track Kids. Period. Full Stop.

Children and teens should not have their online behavior tracked or any other personal information about them collected, profiled, or transferred to other 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 activities in the online and mobile world. 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 collect, store, use, sell, or transfer that information at all. And Congress must pass a law with teeth in order to enforce this prohibition.

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.

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 geolocation services, companies can now also track where kids go in the physical world as well as the virtual one.

Obviously, some online tracking is a helpful aspect of Web 2.0 technology, and parents or teens over the age of 16 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. This is the second major element of a legislative effort to protect the privacy interests of kids.

Because of the dramatic growth of mobile technology and geolocation services, it is absolutely essential that privacy protections apply across all online and mobile platforms. And this Committee and the Senate should pass laws to that effect in this Congress.

Many kids today don’t merely go online – they always are online, whether from their home computer or from a cell phone, iPod, or Web-connected video game console. To reflect today’s mobile and digital world, privacy regulations need to be vastly expanded 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. Geolocation services shouldn’t be allowed without clear prior consent – a formal opt in by a parent – regardless of what type or company or operator provides the service.

It’s important to note that just as we say, “we love media,” Common Sense also loves mobile technology, including for kids, but we are highly cognizant of the downsides as well, especially where the fundamental privacy rights of children and teens are involved.

In April 2010, we published a white paper “Do Smart Phones = Smart Kids? The Impact of the Mobile Explosion on America’s Kids, Families, and Schools.” (*Attached.*)

That paper highlighted the vast expansion of mobile technology usage by kids, and also the ways that smart phones and devices can help kids learn, explore, and engage. But we also highlighted some of the extraordinary potential downsides of mobile media, including ways that these devices may make it easier for kids to engage in inappropriate – and even dangerous – activities. These include cyberbullying, sexting, and distracted driving. Most importantly, Common Sense raised a number of critical questions about the potential downsides of mobile phones and geolocation technology:

Mobile phones with GPS capabilities can expose a kid’s exact location. Many new programs and apps have been developed that allow kids to announce their physical whereabouts. This creates physical safety concerns. If a kid shares location info to “friends,” that information can be passed along to unintended audiences. Privacy concerns are also a huge issue. Marketers use geo-location technology to target kids with promotions. A child’s purchasing habits will be registered and personal data collected. Location-based technology raises several critical questions and concerns:

- Should mobile geolocation data, persistent IP addresses and other identifying information be protected for children under age 13 – in the same way that name, age, gender, and address information are protected today?

(Clearly. And there should be protections for 13 to 17 year olds as well.)

- Do teens understand how their personally identifying information will be used, and do they need additional protections?

(Obviously not, so the privacy of teens must be protected by clear legislation.)

- Will this identifying information be used to target kids and teens with new behavioral advertising and marketing campaigns?

(Sure, unless Congress forbids this practice, as it should.)

There are several additional key principles I'd like to highlight briefly from our recent policy brief, "Protecting Our Kids' Privacy in a Digital World" (*attached*) – which should be essential elements of new privacy legislation from Congress this year.

1. The Industry Standard for All Privacy Should Be Opt In – Especially for Kids and Teens

Companies and operators must make significant changes in the ways that they collect and use personal information. The industry standard should always be "opt in" – 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. And for kids and teens under 16, this means getting their parental permission up front.

Far too many online and mobile companies launch new services – including geolocation-based applications – and enroll users automatically, giving them the opportunity to opt out afterward. This can mean that kids’ personal information is collected and used before the kids or their parents even understand how the service works. All online companies, services, and third-party application providers should follow an industry standard of obtaining a clear opt in, especially for kids.

2. Privacy Policies Should Be Clear and Transparent

Privacy policies must be easy for all users to find and understand and should be carefully monitored and enforced. Instead of lengthy legal documents, companies should use icons and symbols that would clearly and simply convey how – and why – users’ personal information will be used. We need clear, succinct language for privacy policies, especially for kids.

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

Children and teenagers should have the opportunity to delete any and all 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 and teens post personal information on websites, virtual worlds, social networking sites, and many other

platforms. Children also make many mistakes when it comes to their privacy. They should be protected from permanent damage.

Online and mobile companies should be required to 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 tools like “eraser buttons” 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. Congress should require this, and my talented colleagues on this panel should spend some of their companies’ profits to make this a reality.

4. We Must Vastly Increase Education and Information About Online Privacy

Kids and parents need to do their part to protect their online privacy – and the privacy of their friends. A large-scale, multi-year public education campaign will help them learn how to do so effectively. Industry leaders could play a significant role in that campaign, and should be required to finance it.

The online and mobile world is changing so rapidly that children, teachers, and parents all need to be educated about their online privacy rights and needs. Every school in the country should offer a digital literacy and citizenship curriculum, with privacy as an essential component, and this should be funded by industry profits.

Educating and informing consumers is a core element of Common Sense Media’s work. We provide parents and families with reviews of media content, so that they can make informed choices and find media that is appropriate for their children. Recognizing the growing use of mobile devices and mobile apps by kids, Common Sense began reviewing mobile apps last year, and our site now features more than 1,000 reviews of apps for kids. In many cases, our editors and reviewers recommend these apps for kids – but when the apps use geolocation technology to broadcast the user’s physical location, like “Loopt Mix – Chat!”, our reviews make clear that we don’t recommend them for kids, or at least not until they are older teens. But today, there are no required app ratings, and not a single mobile company has taken this issue seriously. Congress should require them to change that reality today.

Balancing Opportunities and Potential Pitfalls

At Common Sense, we recognize that mobile devices and geolocation services can create new opportunities – for learning, exploration, communication, and commerce – for kids and adults. Yet they can also bring enormous threats to our privacy and personal well-being. But whether their impact is positive or negative, mobile phones and devices are not going away. As parents, teachers, industry leaders, and policymakers, we must all take steps to ensure that kids can access the benefits of mobile technology and digital media, while protecting them from potential negative consequences.

Whether our first concern is protecting the best interests of kids and teens, or preserving and expanding a marketplace for all consumers so that tech companies can make profits and

innovate, we all have a role in building a mobile environment that is trustworthy and safe. 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 and extraordinary implications for their privacy. It is time to update our nation's privacy policies for the 21st century. They are terribly out of date. Everyone needs to be a part of this new effort: industry, families, schools, policymakers, and young people themselves. But most of all, this Senate and this Congress need to pass fundamental privacy protections for kids and teens – and their families – now.

Thank you very much.