

February 22, 2010

Rep. Bobby L. Rush
Chairman
Subcommittee on Commerce,
Trade, and Consumer Protection

Rep. Rick Boucher
Chairman
Subcommittee on Communications,
Technology, and the Internet

Congress of the United States
House of Representatives
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

RE: February 24, 2010, testimony at a joint hearing entitled "The Collection and Use of Location Information for Commercial Purposes" before the Subcommittee on Commerce, Trade, and Consumer Protection and the Subcommittee on Communications, Technology, and the Internet

Dear Chairmen Rush and Boucher and Members:

By way of introduction, I am co-director of ConnectSafely.org, founder and executive director of its parent organization, Net Family News, Inc., and currently serving as co-chair of the Online Safety & Technology Working Group, created under the Protecting Children in the 21st Century Act of 2008. ConnectSafely.org is the leading interactive resource on the Web for parents, teens, educators, and everyone engaged and interested in young people's safe, enriching use of the fixed and mobile social Web. Founded in 1999, Net Family News, Inc., is a 501c3 nonprofit organization based in Salt Lake City, Utah, with offices in Salt Lake and Palo Alto, Calif.

Young people's tech-enabled social lives

US teens now send or receive an average of 3,146 text messages a month and 9-to-12-year-olds 1,146, according to the latest figures from Nielsen (<http://bit.ly/d5iiHC>). For them, a text isn't like a phone call, it's part of a conversation as well as of the ongoing flow (or seemingly 24/7 drama) of school life. But texting is only one of young people's social tools. They also use their phones to update their profiles in social network sites,

play games, snap and upload photos to their social network profiles, do the same with videos – and even talk. There is as yet no data on teens' mobile social-mapping or LBS use, but we know that more than 65 million, or about a third, of Facebook users of all ages currently access the social site through their mobile devices ("Online as soon as it happens," February 2010, EU's European Network and Information Security Agency <<http://enisa.europa.eu>>).

In today's fixed and mobile, user-driven media environment, young people's tech-enabled, real-world social lives are highly fluid experiences. They make little distinction between online and offline and fly fast among devices and services. The online and on-phone part are just that – part of and blending into the full picture. Research shows that the vast majority of them – those who aren't already so-called at-risk youth in real life – use technology and devices to socialize with their friends at school and in other important activities and places in their lives. According to the Pew/Internet Project, 91% of teen users of social network sites use them to stay in touch with friends they already see regularly (<http://bit.ly/9cWGZ7>). Technology and Net use simply can't be separated out from their everyday lives (see p. 31, see *Hanging Out, Messing Around & Geeking Out: Kids Living and Learning with New Media*, by Mimi Ito, et al, MIT Press, 2009).

We adults think and talk about stand-alone products and services, such as location-based services (LBSs), each with its terms of use and privacy policy, but it's helpful to keep in mind that young people's tech use is difficult to break down in that way. It's more useful to view the way they use technology in terms of child and adolescent development.

Take today's subject – social mapping or LBS – for example: The use of location-based social networking and games depends on users' mobility and autonomy and has an element of spontaneity. Spontaneous in-person get-togethers are a key purpose of these services – as well as finding good places to eat or drink when you're on your own and new to a city (see New York Times <<http://nyti.ms/3h1gX>>).

A user really needs the independence of an older teen or adult to enjoy BrightKite, Foursquare, or Loopt, for example. The mobility of a driver's license helps

too. What social currency or enjoyment would a 12-year-old get out of posting to his school friends, "I'm at Starbucks with my mom"? He might leave the "mom" part out of it, but his friends, aka social network, probably wouldn't freely be able to act on that announcement because the need for permission or a ride would intervene. Urban youth may have more physical mobility without a driver's license, but there's no reason to believe they have proportionately more freedom from adult supervision.

Meanwhile, location-based services are, to young people, just a new twist on status updates. With 75% of teens owning cellphones (see Pew/Internet, February 2010 <<http://bit.ly/bXjTH3>>), they've for some time had other ways to let each other know their plans and whereabouts: text messages, updates to social-networking profiles, Gmail chat, and instant messages, to name a few. And remember what I said above about who they're using these social tools to send messages to: "each other." "Most teens are not interested in being truly public," social-media researcher Danah Boyd told the Washington Post this month (<http://bit.ly/9MrVKj>). To the extent that LBSs are designed to connect with strangers, most teens are unlikely to use them.

As for youth who don't have engaged caregivers and are reaching out beyond their school-related social circles, there may be a greater degree of risk from LBSs, but this is the demographic that has long represented at-risk youth online, the minority of online youth who need the help of social workers, mental healthcare experts, and risk-prevention practitioners....

Youth risk on the social Web

The most visceral and concerning risk people seem to associate with the collection and use of location data, where minors are concerned, is predation. Research specifically looking at LBSs and predation is needed – and government support of such research would be most welcome – but we already know a lot about youth risk on the Internet in general.

From the significant body of youth-risk research reviewed and presented by the Internet Safety Technical Task Force of 2008 at Harvard's Berkman Center

(<http://bit.ly/by0GRZ>) as well as from subsequent such research, we know that, as far as predation is concerned...

1) Not all youth are equally at risk – the youth most at risk online are those most at risk offline, and a child's psychosocial makeup and home and school environments are better predictors of that risk level than any technology he or she uses.

2) Predation is not the most salient risk online youth face. Mean behavior and bullying by peers are much more common – in fact, two separate national studies have found that about one-third of online youth experience cyberbullying, which is closely associated with what's going at school.

3) The actual risk of Internet-related predation is extremely low, according to Dr. David Finkelhor, director of the Crimes Against Children Research Center at the University of New Hampshire – too low to be estimated in the CACRC's 2000 and 2005 studies of online sexual solicitations of youth. And in a major update last spring ("Trends in Arrests of 'Online Predators'" <<http://www.unh.edu/ccrc/pdf/CV194.pdf>>), he and his co-authors wrote: "There was no evidence that online predators were stalking or abducting unsuspecting victims based on information they posted at social networking sites." [Note that much of the geolocation information under discussion, here, as being posted via location-based apps, games, and services is being posted to social networking sites.]

For context: We have also long known that the vast majority of sexual exploitation cases against children are perpetrated by people they know in everyday life *offline*; a less-well-known fact is that between 1990 and 2005, when the World Wide Web got its start and grew exponentially, there was a 51% decline in overall child sexual exploitation, and the latest FBI figures show a continuing drop in violent crimes ("2008 Crime in the United States" <<http://bit.ly/dBVIPy>>). The number of rape cases is down 9.6% since 2004, "considerably more of a decline than the overall crime drop during this period," Dr. Finkelhor reported last September. He explained how that spells a decline in child sexual abuse: "While there is no specific child victimization category, bear in mind that well over half of the rapes known to law enforcement are against persons under 18,

so this rape decline is very much a drop in child victimization" (Finkelhor in an email to a group of youth-risk practitioners, researchers, and NGOs).

Apart from the unlikelihood of minors using LBSs when they don't have the means independently to meet up with friends in real time (as mentioned above), the research also shows they are psychosocially disinclined to interact with people who aren't friends and known peers and who aren't part of the flow of their social experience at any given moment. A recent study of how youth deal with strangers in a social network site – which, like texting, is part of their social flow – found that 92% of youth at the receiving end of sexual solicitations in a social site either had an appropriate reaction or ignored the solicitation ("The Association of Parenting Style and Child Age with Parental Limit Setting and Adolescent MySpace Behavior," by Dr. Larry Rosen, in *Journal of Applied Juvenile Psychology*, November-December 2008 <<http://bit.ly/bfs3vP>>). ["Appropriate reaction" was defined as telling the person to stop, blocking the person from their page, removing themselves from the situation by logging off, or reporting the incident to an adult or to the site.]

As for LBSs themselves, it is my understanding that most of the new social-mapping services do not involve automatic, software-produced disclosure of the cellphone owner's movements, but rather disclosure by the user himself of his whereabouts, in the form of a social-networking-style update. If there are concerns about what minors post about their location via LBSs, the concerns would necessarily also apply to other social-media services, including instant messaging, Skype, Facebook, Twitter, and texting on mobile phones. LBSs by themselves do not represent a unique safety threat. [PleaseRobMe.com, an awareness-raising site, points out that sharing one's location widely when not at home potentially lets burglars know one's house is up for grabs, but this is a risk to adults' property not to youth safety.] We are concerned about children who do download LBSs being bombarded with advertising and marketing based on their location and hope proliferating geolocation-enabled apps are informed about and operate in compliance with the Children's Online Privacy Protection Act.

The question has been asked whether the way LBSs function is too complex for young people to grasp. My answer is that they are no more complicated to use than

Facebook or MySpace and much less complex than a console videogame or multiplayer online game like World of Warcraft. We also know from a December 2008 study by Computer Associates that social sites' privacy features are not too difficult for teens to use, and teens do use them; the study showed that 79% of teen social networkers restrict access to their profiles in some way (<http://bit.ly/7bRb>). That is not to say that all users, including the relatively few teens likely to be using LBSs, will not need plenty of consumer education and sound notice-and-consent practices on the part of location-based providers concerning the wider dissemination of their posts through networks these services are connected to such as Facebook and Twitter. In other words, it's more important than ever that LBSs follow CTIA's guidelines for customer notice and consent and that all parties, from app developers to service providers, are committed to clear notice to and consent by consumers as to how their location information is being used.

Protecting a moving target

How to protect young people in a user-driven media environment in which youth define active use (see "Generation M2" from the Kaiser Family Foundation <<http://bit.ly/7XukS3>>) has been a puzzle since the advent of interactive media. First we thought we should figure out how to protect them from technology, since technology was "obviously" the main problem. Then we learned from the growing bodies of both youth-risk and social-media research that the main "problem" is actually child and adolescent development and behavior. Adults not up to speed on the research keep thinking that regulation must be a solution, and as a society we have struggled to enact legislation that could somehow protect both children and free speech, when it increasingly seems impossible to define, separate out, and control inappropriate adolescent behavior while somehow leaving alone what is appropriate, developmentally normative, and constructive.

Meanwhile, 1) social media and technologies continue to proliferate, 2) the Internet becomes increasingly accessible, 3) young people's social lives are increasingly a mashup of online and offline experiences and of new media, technologies, and devices,

and 4) young people keep growing and maturing (an obvious fact that often somehow gets left out of the equation). Change – in technology, media, households, consumer behavior, unfolding research, and individual kids – truly is the only constant in this scene.

Consumer education + best practices + parental-control tools

Regulation is a blunt instrument in the face of this level of fluidity and change, micro and macro. Only the caring adults closest to a child can possibly know how to calibrate family rules and parental-control tools to fit a growing child's needs.

The ultimate protection for all children is the filtering "software" in their heads. It has numerous benefits: Every child is born with this latent filter, which improves with use, works with all devices, and is with her wherever she goes. Its downside is that children need help in developing their cognitive filter, and not all "developers" – parents, caregivers, educators, etc., teaching them media and life literacy – understand the ever increasing importance of this filter and the responsibility its owner and they have in developing it.

In other words, consumer education – for youth, parents, and schools – is not only essential but becoming increasingly more so. Its most basic and vital forms are the new media literacy and citizenship that help children's cognitive filter think critically about what's going out (behavioral and informational) as much as what's coming in as they use two-way social, or behavioral and collegial, media. This kind of literacy gets developed largely at home and school from the earliest ages, when children first use technology. But consumer education takes many other forms as they grow, forms that are just as important: from notice & consent in LBSs to tutorials for features in products and services to professional development for educators about teaching with new media. Children's education needs to be provided by parents, industry, government, and schools; *parent and educator* consumer education needs to be provided by NGOs, industry, and government.

Children can't learn how to use social technology and media properly without having access to these new media and technologies – just as swimming can't be taught without pools – so government and other entities need to join industry in promoting their

wise use in US education and ending efforts to block them. This is becoming widely recognized overseas – see British education watchdog Ofsted's February 2010 report <<http://bit.ly/aPR298>> showing that schools rated "outstanding" for online-safety conditions and instruction used "managed" rather than "locked down" filtering, thereby requiring pupils to learn how to "take responsibility themselves for using new technologies safely."

Supporting that all-important education is a key industry best practice, which needs the support of government. For example, the wireless industry association is currently revising its best-practice guidelines, appropriately broadening the definition of location-based services. It is also working on a consumer-education campaign to increase public awareness of parental controls and other options parents have to support children's safe, constructive use. We recommend that the industry also mount an education program aimed at both parents and youth which is focused specifically on location-based services, games, and apps – so they understand how to use privacy features and who might see the location information they're disclosing.

Another important support to parents as they protect and educate their children are a broad variety of parental-control tools to choose from as their children mature. The mobile carriers provide a robust array of such tools, from time limits on devices to caller blocking to restricting app downloads. That last control is an excellent protection against minors using LBSs not appropriate for their use. The main current provider of cellphone apps, Apple, rates apps by age and provides parental controls for its iPhone and iPod Touch (though without much transparency to consumers and NGOs) in addition to the Smart Limits parental controls provided by iPhone service provider AT&T. NGOs, industry, and government need to work together to raise consumer awareness of these protective tools and features. An excellent recent example of government-NGO partnership is the Federal Trade Commission's NetCetera booklet and campaign. We'd like to see more coordination within the US government and between government, industry, and NGOs along the lines of the UK's Council for Child Internet Safety (<http://www.dcsf.gov.uk/ukccis>).

Conclusion

There is risk to using LBSs for youth, just as there is to their using any means to interact with the world – but mostly in the area of peer-to-peer interaction, where tech-based socializing is concerned. Teens use text messaging, talking, instant messaging, social networking, and other social tools to notify friends of their thoughts, plans, and whereabouts. We do not see LBSs as representing greater risk than other social media, particularly to youth under 16, because independence and mobility are basic criteria for enjoying the services. At the same time, the research shows that teens who are not taking extraordinary risks in the real world are savvy about ignoring or appropriately reacting to overtures from strangers, and that the risk of "online predators victimizing unsuspecting teens because of information they're posting in social sites" is not evident to the Crimes Against Children Research Center.

It's useful, especially since there is no research specific to minors' use of LBSs, to view their use in the context of young people's use of all social media and technologies, as well as in the context of the everyday, tech-enabled social lives of today's teens. Technology and Net use simply can't be viewed as separate from the flow of their online/offline social lives. With these social technologies, the research shows, the vast majority of youth are socializing with friends and peers at school.

To remove the risks associated with their social lives, online and offline, is not only impossible but harmful to their development, as risk assessment is a primary task of adolescent development, pediatricians and child-development specialists tell us. Legislating against youth risk is not the answer. A combination of parental-control technologies, industry best practices, more consumer education, and better coordination of efforts to protect youth both within the federal government and in cooperation with industry and NGOs is the best way to go.

ADDENDUM A

Right after I filed the above written testimony, a colleague "tweeted" about a new blog post by a parent about Google Buzz. Because Buzz is brand-new and a hybrid of LBSs, Gmail, micro-blogging, and social networking, we're all at the early stages of figuring out its implications for kids, a lot of whom are known to use Gmail (I haven't been able to find numbers).

The parent is social-media industry analyst Charlene Li. She blogged on Sunday (<http://bit.ly/aARahl>) that her 9-year-old daughter quickly figured out how to use Buzz (from her computer), enjoyed it, and had had one conversation on it with her friends. The problem was that her daughter and friends didn't know that the conversation wasn't visible only to them. It was a public conversation.

Li writes that "the easiest thing to do as a parent is to simply disable Buzz, meaning that the Google profile and all followers are deleted – permanently." But because her daughter enjoyed Buzz so much, she seems open to "managing groups, privacy settings, etc." so her child can continue using the service. "We'll give it a try," she writes, "but unless her friends also keep the conversation private, it will all be for naught." Ensuring that with the other kids in the group and their parents will be a project.

Google last summer agreed, in response to a complaint by the Children's Advertising Review Unit of the Better Business Bureau, a COPPA Safe Harbor, to require a birth date at registration to Gmail and, if a user indicates he or she is under 13, a session cookie to block the user from re-registering with an earlier birthdate.

That's a start, but what this issue points to is the impact on children's privacy of *combining* social-media products within companies and connecting them across networks such as Facebook Connect. Perhaps the FTC's forthcoming review of COPPA rules and enforcement will address this emerging issue. But we feel the brilliant software engineers and project managers who develop these products need to wear their parent hats more, companies need to be thinking through children's privacy from the earliest development stages, and industry best practices need special sections or clauses addressing child privacy and safety.

–Anne Collier, *ConnectSafely*

ADDENDUM B

ConnectSafely.org's Cellphone Safety Tips (<http://bit.ly/9W4jBf>)

Cellphones are increasingly full-blown handheld computers, and everything that can be done on the Web via computer – photo-sharing, Web browsing, game playing, tune-swapping, real-time text chat, and (oh yeah) talking – can be done on a phone. Here are some basic ideas for keeping mobile phone use safe and constructive:

Smart socializing. Use the same good sense about what you post from your phone as from a computer. Once they're posted, text, photos, and video are tough to take back, can be copied and pasted elsewhere, and are up there pretty much forever. Think about the people in them (including you!). Reputations are at stake – even more so if nudity or sex is involved.

Phones are personal. Letting other people use your phone when you're not around is like letting them have the password to your social network profile. They can impersonate you. Which means they can play tricks on you that could really become a problem. It's a good idea to lock your phone when you're not using it. It's not a good idea to let friends text for you while you're driving. Don't text while driving; just be safe and turn the phone off!

Bullying by phone. Because people socialize on cellphones as much as online, cyberbullying can be mobile too. Treat people on phones and the Web the way you would in person, and the risk of being bullied goes down. Be aware, too, of people randomly taking pictures at parties – you may not want to be tagged in their social-network photo albums.

Sexting: It's the same on phones as on the Web - do not take, send, post or even store on your phone nude photos of anyone under 18. You could be charged with production, distribution, or possession of child pornography, a serious crime. You could also be subjected to jokes, bullying, blackmail, expulsion from school, loss of a job, etc. and the images can circulate forever.

The value of "presence." If you do a lot of texting, consider the impact that being "elsewhere" might be having on the people around you. Your presence during meals, at parties, in the car, etc. is not only polite, it's a sign of respect and appreciated.

Down time is good. Constant texting and talking can affect sleep, concentration, school, and other things that deserve your thought and focus. You need your sleep and *real* friends understand there are times you just need to turn off the phone - harassment can happen between midnight and morning too.

Social mapping. Most cellphones now have GPS technology and there are a growing number of services that allow friends to pinpoint each other's physical location. If you use such a service, do so only with friends you know in person, and get to know the service's privacy features!

ConnectSafely.org's Social Web Safety Tips for Teens (<http://bit.ly/aGQG8z>)

*These tips, based on the latest research, will help teens' socializing stay fun and safe on both the fixed and mobile social Web. **Be your own person.** Don't let friends or strangers pressure you to be someone you aren't. And know your limits. You may be Net-savvy, but people and relationships change, and unexpected stuff can happen on the Internet.*

Be nice online. Or at least treat people the way you'd want to be treated. People who are nasty and aggressive online are at greater risk of being bullied or harassed themselves. If someone's mean to you, try to ignore them - often that makes them stop. Use privacy tools to block them from viewing your full profile and contacting you.

Think about what you post. Sharing provocative photos or intimate details online, even in private emails, can cause you problems later on. Even people you consider friends can use this info against you, especially if they become ex-friends.

Passwords are private. Don't share your password even with friends. It's hard to imagine, but friendships change and you don't want to be impersonated by anyone. Pick a password you can remember but no one else can guess. One trick: Create a sentence like "I graduated from King School in 05" for the password "IgfKSi05."

Read between the "lines." It may be fun to check out new people for friendship or romance, but be aware that, while some people are nice, others act nice because they're trying to get something. Flattering or supportive messages may be more about manipulation than friendship or romance.

Don't talk about sex with strangers. Be cautious when communicating with people you don't know in person, especially if the conversation starts to be about sex or physical details. Don't lead them on - you don't want to be the target of a predator's grooming. If they persist, call your local police or contact CyberTipline.com.

Avoid in-person meetings. The only way someone can physically harm you is if you're both in the same location, so – to be 100% safe – don't meet them in person. If you really have to get together with someone you "met" online, don't go alone. Have the meeting in a public place, tell a parent or some other solid backup, and bring some friends along.

Be smart when using a cell phone. All the same tips apply with phones as with computers. Except phones are with you wherever you are, often away from home and your usual support systems. Be careful who you give your number to and how you use GPS and other technologies that can pinpoint your physical location.

ConnectSafely.org's Social Web Safety Tips for Parents (<http://bit.ly/4zUOR3>)

These tips for parents about safety on the social Web are based on the latest research from the Crimes Against Children Research Center at the University of New Hampshire (with input from our colleagues there).

Be reasonable and try to set reasonable expectations. Pulling the plug on your child's favorite social site is like pulling the plug on his or her social *life*. Instead of being protective, it can shut down communication and send kids "underground" where they're more at risk. It's too easy for them to set up free blogs and profiles from anywhere, including friends' houses or even a cell phone.

Talk with your kids about how they use the services. They, not news reports or even experts, are the ones to consult about their social-Web experience. Help them understand basic safety guidelines, such as protecting their privacy (including passwords), not harassing peers, never talking about sex with people they don't know, avoiding in-person meetings with people they "meet" online, and taking care in what they post - because anything people put online can be grabbed, reworked, and used against them.

Support critical thinking and civil behavior because no laws or parental-control software can protect better than a child's developing good sense about safety and relationships. Research shows that kids who are aggressive and mean online toward peers or strangers are at greater risk of becoming victims themselves. So teach them to be good citizens and friends online as much as offline.

Consider requiring Internet use in a high-traffic place in your home - not in kids' rooms - to help you stay aware of their online time. This way, you can encourage a balance between online time and their offline academic, sports, and social times. Know that there are also many ways kids can access the Internet away from home, including on many mobile phones and game players.

Try to get your kids to share their profiles and blogs with you, but be aware that they can have multiple accounts on multiple services. Use search engines and the search tools on social-networking sites to search for your kids' full names, phone numbers and other identifying information. You're not invading their privacy if they're putting personal info in public "places" online. If their pages are private, that's a good thing, but it's even better if they share it with you.