The New Children's Online Privacy Rules

What Parents Need to Know

June 2013

Center for Digital Democracy | DemocraticMedia.org

THE NEW CHILDREN'S ONLINE PRIVACY RULES: WHAT PARENTS NEED TO KNOW

Beginning on July 1, 2013, parents will have new tools to protect their children's privacy on the Internet, social media, iPads or tablets, mobile phones, and interactive games. The Federal Trade Commission (FTC) has just updated its rules under the Children's Online Privacy Protection Act (or COPPA), giving parents greater rights – and responsibilities – for guiding their children's use of digital media. This primer is designed to help parents understand and use the new rules to help their families.

WHY COPPA WAS ENACTED & WHAT IT DOES

In the mid-90s, children's media advocacy groups became increasingly concerned as dozens of companies began setting up websites for kids that offered prizes and other incentives to encourage children to supply personal information about themselves. The sites were based on a whole new approach to advertising made possible by the interactive nature of the Internet. It was called "one-to-one" marketing. At its core was data collection. Children, who were excited by the new online experience, were seen as easy targets.

One site aimed at "young investors," urged children to provide an astonishing amount of financial information, including any gifts they might have received in the form of stocks, cash, savings bonds, mutual funds or certificates of deposit.

> "Children… were seen as easy targets."

Another site, set up to promote the movie Batman, encouraged children to "be good citizens of Gotham" and fill out the "census."

Unlike television, where there were guidelines for advertising to children, the Internet had no such rules. After a 3-year campaign by a broad coalition of child advocacy, privacy, and consumer groups, Congress passed the Children's Online Privacy Protection Act in 1998 to establish "rules of the road" for companies targeting children on the World Wide Web.

COPPA took effect in 2000. Because the law was based in decades of scientific research documenting young people's developmental vulnerabilities to the persuasive techniques of advertisers, its key goals were to prevent online companies from targeting individual children with personalized marketing messages, and to put parents in control of what information is collected from their young children. COPPA applies to websites that are directed to children under the age of 13. Its basic requirement is that operators

of child-oriented websites cannot solicit personal information from children without notifying and seeking permission from their parents in advance. These regulations have helped create a safer, secure, and more responsible online environment for children.

GROWING PRIVACY THREATS IN THE ERA OF "BIG DATA"

In the fifteen years since passage of this important law, the Internet has changed dramatically. Today's children are growing up in a powerful, always-on media culture. They are engaging with new media technologies at much earlier ages – many during their toddler years. As "digital natives," they are spending increasing amounts of time playing, interacting with friends, gaming, using mobile apps, and posting content on social media. This new media culture has also become highly commercialized. Children remain a valuable target market for advertisers. They not only spend their own money, but they also prod their parents – through the so-called "nag factor"– into buying particular brands, even for family purchases like cars and other big-ticket items. In all, children spend or influence $1.2 trillion per year.

"Children spend or influence $1.2 trillion per year."

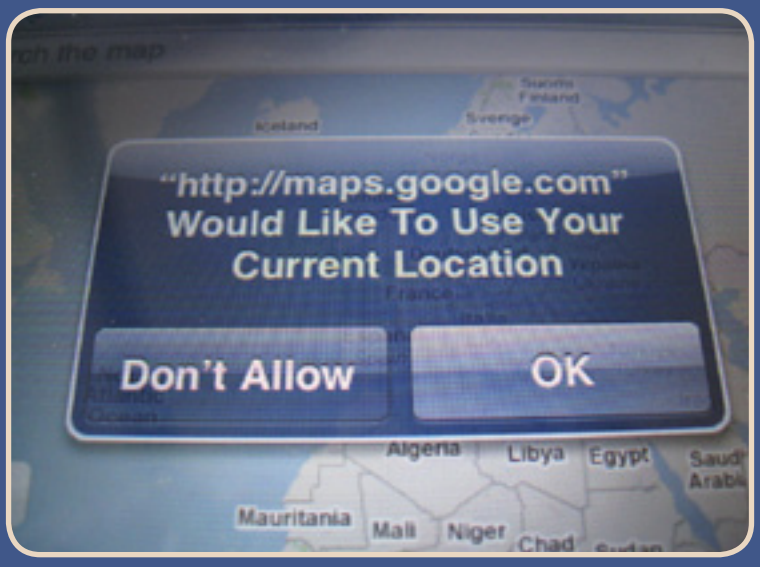
Advertising on digital media is a far cry from the more familiar commercials that interrupt children's TV programs. Marketing is now woven into the very fabric of young people's daily experiences, following them wherever they go on a 24/7 basis. As a consequence, children are increasingly exposed to a flood of new digital marketing and data collection techniques designed to track, target, and influence them.

In this new era of "Big Data," what people voluntarily say about themselves online is only part of the massive amount of information that is gathered on them, much of it without their knowledge. Many parents may not realize that deeply embedded in our mobile apps, online games, and social media are a growing number of largely invisible tracking

technologies that spy on us and our children, compiling extensive databases, and routinely sharing massive information with numerous companies and other third parties – sometimes even with government agencies. Here are just a few of the ways that digital marketers can track and target individuals:

- **They can follow us wherever we go through our mobile phones.** As more and more of us rely daily on our mobile phones, companies now have a way to track our precise locations throughout the day – including what we do while we are there – and identify behavior patterns unique to each of us. This information can then be used to target us through geolocation marketing techniques. For example, fast food marketers can reach us as we walk past a restaurant and send targeted messages directly to our phones, enticing us to come in.

- **They are monitoring our friendships and social relationships.** Through social media, interactive games, and mobile apps, marketers are also collecting information about who our friends are, the nature of our relationships, and how we interact with them. Using influence marketing on social media, companies enlist many of us to promote brands to our friends and acquaintances, either by encouraging us to "like" products, or by posting our actions – where we go, what we buy, and what media we consume – on our friends' newsfeeds.



- **They are compiling personal profiles based on online and offline information.** Marketers are using elaborate software programs that can compile highly detailed profiles on each of us, combining what is collected online and through our mobile phones with information from data brokers. In addition to our age, gender, where we shop and what we buy, these profiles can include such things as our ethnic background, any health issues we have, and our political affiliations.

- **They don't need to know our names to know who we are, where we are, and how to reach us.** With the increasing use of personal digital devices such as smart phones and Internet-enabled gaming consoles – which are associated with individual users, rather than families –marketers do not need to know our name, address, or email in order to identify, target, and contact us.

- **They are perfecting ways to manipulate our behaviors.** With the growth of sophisticated software, marketers can create personalized messages designed to tap into our own particular behaviors, interests, and vulnerabilities. Companies can insert these messages directly into our online, mobile, and gaming experiences, using special tools that monitor our responses in "real time" and alter the marketing content to make it more effective.

These practices are widespread and largely invisible. They are worrisome enough for adult consumers. But when they are used to target and influence children, they are particularly troubling. Children under 13 are still developing – psychologically, biologically, and socially. They often don't completely understand when someone is

trying to persuade or manipulate them. The younger ones can't always tell the difference between fantasy and reality, or recognize advertising. Even older children can be fooled by advertising, especially if it is disguised as entertainment, embedded in an online game, or presented to them through a friend. As kids grow into their pre-teen years, they become more influenced by their peers and can be persuaded to do risky things without realizing what the harms may be. They are inclined to behave impulsively and often don't think about the consequences of their actions before taking them. As they begin to explore their identities, they are increasingly drawn to social media, posting photos and other personal information about themselves, and not always using good judgment about what they share.

THE NEED FOR UPDATED RULES

A recent survey conducted by the Center for Digital Democracy (CDD) and Common Sense Media found that many parents are concerned about the new marketing and data collection practices that companies are using to target their children:

- **91%** of both parents and adults believe it is not okay for advertisers to collect information about a child's location from that child's mobile phone.
- **96%** of parents and 94% of adults expressed disapproval when asked if it is "okay OK for a website to ask children for personal information about their friends."
- **94%** of parents, as well as 91% of adults, believe that advertisers should receive the parent's permission before putting tracking software on a child's computer.

Although COPPA has continued to offer some protections for children in the expanding digital marketplace, child advocates, privacy groups, and health experts have been urging the government to revise the regulations to ensure they will be effective in light of the growing set of techniques that today's marketers are using. Now, after more than two years of public workshops, Congressional hearings, input from a wide variety of stakeholders, and negotiations with the public interest community and industry, the Federal Trade Commission has released a new set of updated regulations.

WHAT THE NEW RULES SAY

The new rules refine and clarify COPPA's basic safeguards for putting parents in charge of what personal information can be collected from their children. The FTC has also added new protections specifically designed to address a wide range of platforms and practices that are becoming state-of-the-art in today's contemporary media culture.

- **COPPA's safeguards** now cover a wide range of digital media that a child regularly encounters – from social networks to Internet-enabled gaming devices to mobile apps.

- **Personal information** now includes much more than a child's name, address, or email, covering a variety of ways that companies could use to identify and contact individual children:

    - Geolocation such as street address and city that can be collected through the mobile phone or other mobile device;

    - Photos or videos a child posts with images of herself, as well as audio recordings with the child's voice;

    - "Cookies" and other hidden software – called persistent identifiers – that online companies use to track an individual child's behavior and movements on digital media;

    - A screen name or user name – if that name could be used to re-contact the child directly.

WHAT THE NEW RULES SAY (CONTINUED)

- **A children's website, mobile app, or game** is required to ask parents in advance and get their permission before collecting any of these types of information from children.

- **These companies must also include links to a privacy policy**, not only on their home page, but also everywhere on their site (or digital service) where personal information is collected from children. The link must be prominently displayed so it is easy to find. The privacy policy must explain in clear language what kinds of information the site collects, how the information is used, and whether it is shared with other companies. Some children's online content providers allow other companies to collect personal information from a child visitor. In these cases, the names of the companies collecting this information must be disclosed as well.

- **In order to ensure that the company is actually obtaining consent from the parent**, and not from the child herself or someone else, parents may be asked to sign a consent form, provide some kind of verifiable ID, or – in limited cases – send an email. However, companies may not ask you for your credit card information unless you are also buying something for your child.

- **If a child has provided personal information to a website or online service without a parent's permission**, that parent has the right to receive from the company a description of what has been collected, to refuse to permit further use or collection of the child's personal information, and to delete information that has already been collected.

- **While companies can still place advertising and marketing on child-directed websites or other digital media**, there are important new restrictions on advertising messages that are tailored to an individual child. Such forms of behavioral advertising, as well as retargeting (where a marketer follows someone and keeps sending them personalized messages) can be especially manipulative when used with children, and are no longer permitted without parental notice and consent.

SOME TIPS FOR PARENTS

- **Talk with your children** about what they do and where they go online, as well as what apps they download on their mobile phones. Make sure that the media they are engaging with is age-appropriate.
- **Explain to them** that they need to be very careful about what they post online about themselves. They should never post photos, videos, their email address, telephone number, or other identifying information about themselves without first asking for parental permission.
- **Be wary** of websites, mobile apps, and other child-oriented digital media that ask for a lot of personal information that does not seem necessary. Companies shouldn't have to collect huge amounts of information about your child in order to provide an entertaining or educational experience.
- **Be especially careful** about your children's use of mobile phones.
  - Mobile apps should never ask your child to give permission for collection of her location without first obtaining your permission.
  - When downloading apps for your children, be aware that app providers are not required to explain what personal information is collected from children at the time you decide to purchase the app. However, notification must appear on the landing page once the app has been downloaded. This puts added responsibility on parents to look at the app that a child is about to use and to decide if they are comfortable with the child using that app.
  - Keep in mind that some apps may be "free" to download, but once children begin playing with them, they may be prompted by the app to purchase multiple items in the game ("virtual goods"), in order to gain advantages or move up to various levels. This practice – which is becoming a dominant business model for interactive games and apps – can rack up a very high bill without parents even knowing.
- **Review the privacy policies** of all the websites and digital devices your children use to make sure you are comfortable about the safety, security, and privacy protections provided on them.

If you believe a company is violating the new COPPA rules, you can contact the Federal Trade Commission directly at **COPPAhotline@ftc.gov**.

The Center for Digital Democracy has been the lead group in Washington pushing for these safeguards. We are here to continue that fight, help parents hold the children's media and marketing industries accountable, and encourage responsible practices for protecting our youth.