



Protecting Kids' Privacy Online

**Final Amended COPPA Rule
effective July 1, 2013**

COPPA Background

- **Goals:**
 - Permit parents to make informed choices about when and how children's personal information is collected, used, and disclosed online; and,
 - Enable parents to monitor their children's interactions and help protect them from the risks of inappropriate online disclosures.
- COPPA is the only child-specific federal privacy law in the United States.

Basic Requirement

- Operators of commercial websites and online services must provide **NOTICE** and obtain parents' **CONSENT** before collecting personal information from children under age 13.

Changes to the Rule

- Definitions
- Online and Direct Notices
- Parental Consent Mechanisms
- Confidentiality and Security of Children's PI
- Data Retention and Deletion
- Safe Harbor Programs
- New Voluntary Processes for FTC Approval

What is a website or online service under COPPA?

- Website: content that users can access through a browser on an ordinary computer or mobile device
- Online service: covers any service available over the Internet, or that connects to the Internet or a wide-area network. Includes:
 - Mobile applications that send or receive information over the Internet and that allow children to: Play network-connected games, Engage in social networking activities, Purchase goods or services online, Receive behaviorally targeted advertisements, Interact with other content or services
 - Internet-enabled gaming platforms
 - Voice-over-Internet protocol services
 - Internet-enabled location based services

Who must comply with COPPA?

- Commercial websites and online services **directed to children** that collect, maintain, or provide the opportunity to disclose personally identifying information or “PII.”
- Operators of **general audience** sites and services (including teen/tween sites) who have **actual knowledge** that they collect kids’ PII.
- Entities on whose behalf operators collect the information.

“Operator” (revised)

- Personal information is collected or maintained on behalf of an operator when:
 - it's collected or maintained by the operator's agent or service provider; or
 - the operator benefits by allowing another person to collect PI directly from its users.
- Applies to 1st party child-directed sites/services that embed 3rd party content

“Directed to Children” under COPPA

(Revised)



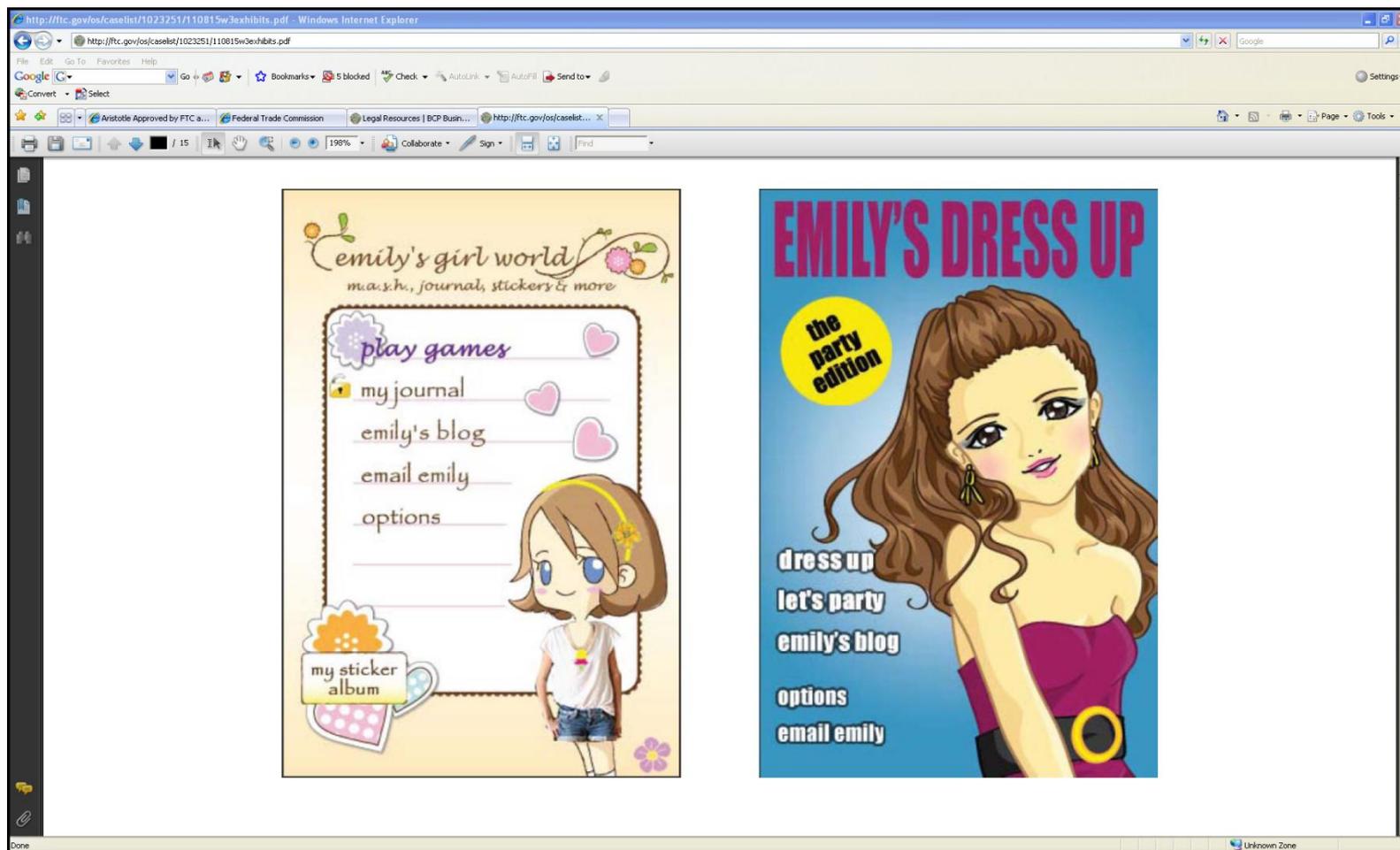
FTC considers several factors, including:

- Subject matter, content, animated characters, age of models, language, graphics, activities, or incentives, music, presence of child celebrities or celebrities appeal to children;
- Whether advertising promoting or appearing on the site or service is directed to children;
- Evidence about intended audience;
- Empirical evidence about audience composition.

“Website/Online Service Directed to Children” (revised)

- Reorganized definition sets out criteria for site/service directed to children upfront
- Adds provision that a service collecting PI directly from users of child-directed site/service is covered where it has *actual knowledge* of such collection;
 - Applies to 3rd party services embedded on child-directed sites/services
- Adds provision allowing child-directed site/service, which doesn't target children as its *primary* audience, to age-screen to provide COPPA protections only to users under 13

“Directed to Children” under COPPA



General Audience under COPPA

- Must have **actual knowledge** that they collect personal information from children.
- “Actual knowledge” can come from asking a child’s age, grade, birthday, other age-identifiers. May also come from notification from a concerned parent or other individual.

“Personal Information”

- Full name
- Physical address
- Online contact information,
- Screen or user name **where it functions like online contact information**
- Telephone number
- Social Security Number
- Information concerning the child or parents combined with another identifier

“Personal Information”

Updates to the Definition of PI:

- **Persistent identifiers** (e.g., cookie strings, user IDs, IP addresses, processor or device serial numbers, unique device identifiers) used to recognize a user over time and across different websites or online services;
- **Geolocation information** sufficient to identify street name and name of city/town;
- **Screen/user names** where they function in the same manner as online contact information; and
- **Photos, videos, or audio files** containing a child’s image or voice.

“Collects or Collection”

- Requesting, **prompting, or encouraging** that children submit personal information online, even when optional.
- Enabling children to make the information public, e.g., in a chat room or profile.
- Passive tracking linked to personal information.

Revised Rule modifies part (2) of definition to:

- Replace the “100% deletion standard” with a “reasonable measures” standard
- Let operators provide interactive communities for children without parental consent as long as they take reasonable measures to delete *all or virtually all* children’s PI before it’s made public.

“Collects or Collection”

Modifies part (b) of definition to:

- Replace the “100% deletion standard” with a “reasonable measures” standard.
- Let operators provide interactive communities for children without parental consent as long as they take reasonable measures to delete *all or virtually all* children’s PI before it’s made public.

“Support for Internal Operations” (New)

- Includes use of persistent identifiers to:
 - Maintain/analyze functioning site/service
 - Perform network communications
 - Authenticate users/personalize content on site/service
 - Serve contextual advertising, cap frequency of ads
 - Protect security/integrity of site/service
 - Ensure legal/regulatory compliance
- Excludes use of persistent identifiers for behaviorally targeting or amassing a profile on a child or for any other purpose

Under COPPA, Operators Must:

- Post a **privacy policy** and links to the policy wherever personal information is collected.
- Give parents **direct notice** of its information practices.
- With certain exceptions, obtain **verifiable parental consent** before collecting information.

Notices (Revised)

- Improves the “direct notice” to:
 - Ensure that key information is presented to parents in a succinct “just-in-time” notice;
 - Provide a clear roadmap for operators as to content of direct notice depending upon its collection and use practices.
- Streamlines the privacy policy by requiring a simple statement of:
 - The information the operator collects from children, including whether the website/online service enables a child to make PI publicly available;
 - How the operator uses such information; and
 - The operator’s disclosure practices for such information.

Parental Consent

Must be reasonably calculated, **in light of available technology**, to ensure:

- The parent child receives **NOTICE** of the operator's practices regarding the collection, use or disclosure of the child's personal information.
- The person providing **CONSENT** is the child's parent (or legal guardian).
- New technologies may satisfy this requirement.

Parental Consent

Updates ways to obtain verifiable parental consent by adding certain approved methods:

- Electronic scans of signed parental consent forms,
- Video-conferencing;
- Use of government-issued identification checked against a database, provided that the parent's ID is deleted promptly after verification;
- Use of debit card or other online payment system, if it provides notification of each transaction;
- Retains “email plus” for internal uses of PI.

Parental Consent

To encourage development of new consent mechanisms, adds 2 procedures for approval:

- Commission approval: Establishes a voluntary 120 day notice and comment process for parties seeking FTC approval of a particular consent mechanism.
- Safe Harbor approval: Permits operators participating in an FTC-approved safe harbor program to use a method permitted by that program.

Exceptions to Parental Consent

Adds 3 new exceptions:

- Where site/service collects parent's online contact information (but no other PI from child) to keep parent informed of a child's activities;
- Where site/service collects persistent identifier (but no other PI from child) for sole purpose of providing "support for internal operations";
- Where plug-in collects persistent identifier on a child-directed site/service (but no other PI) from a 13+ previously registered user.

Under COPPA, Operators Also Must:



- Provide parents **access** and opportunity to **delete** child's personal information and opt-out of future collection.
- **Limit collection** of personal information.
- Ensure **confidentiality, security, and integrity** of personal information.

Data Security (Revised)

Strengthens the Rule's confidentiality, security, and integrity provision by:

- Adding a requirement that operators take reasonable steps to release children's PI only to parties capable of maintaining its security.

Adds a data retention and deletion provision to:

- Retain children's PI for only as long as is reasonably necessary to fulfill the purpose for which it was collected; and,
- Properly delete PI by taking reasonable measures to protect against unauthorized access to or use in connection with its deletion.

Voluntary Approval Processes

- **Parental consent methods:** Request for Commission approval of new mechanisms
- **Support for internal operations of the website or online service:** Request for Commission approval to add new activities to the definition of support for internal operations
- All requests published for public comment
- Commission determination within 120 days of request

Self-Regulatory Safe Harbor Programs under COPPA

- There are 5 approved safe harbors:
 - Aristotle, Inc. www.aristotle.com/integrity
 - CARU www.caru.org
 - ESRB www.esrb.org
 - Privo, Inc. www.privo.com
 - TRUSTe www.truste.com
- An operator participating in and complying with an FTC-approved safe harbor will be deemed to be in compliance with the Rule.

Safe Harbor Programs

Strengthens COPPA safe harbors by requiring them to:

- Detail their business models and technological capabilities and mechanisms to assess and insure members' COPPA compliance;
- Audit members at least annually;
- Report to the Commission (July 1, 2014 and annually thereafter) on the aggregated results of internal audits; and,
- Submit revised guidelines on March 1, 2013 or their approval will be revoked.

COPPA Enforcement

- Agency has filed **19** federal court actions, and has obtained **over \$6.6 million** in civil penalties.
- FTC is authorized to seek up to **\$16,000/violation** in penalties
- Deletion of personal information collected without parental consent;
- Employee education and written acknowledgement;
- Written compliance report to FTC; and
- Consumer education.

Educating Consumers



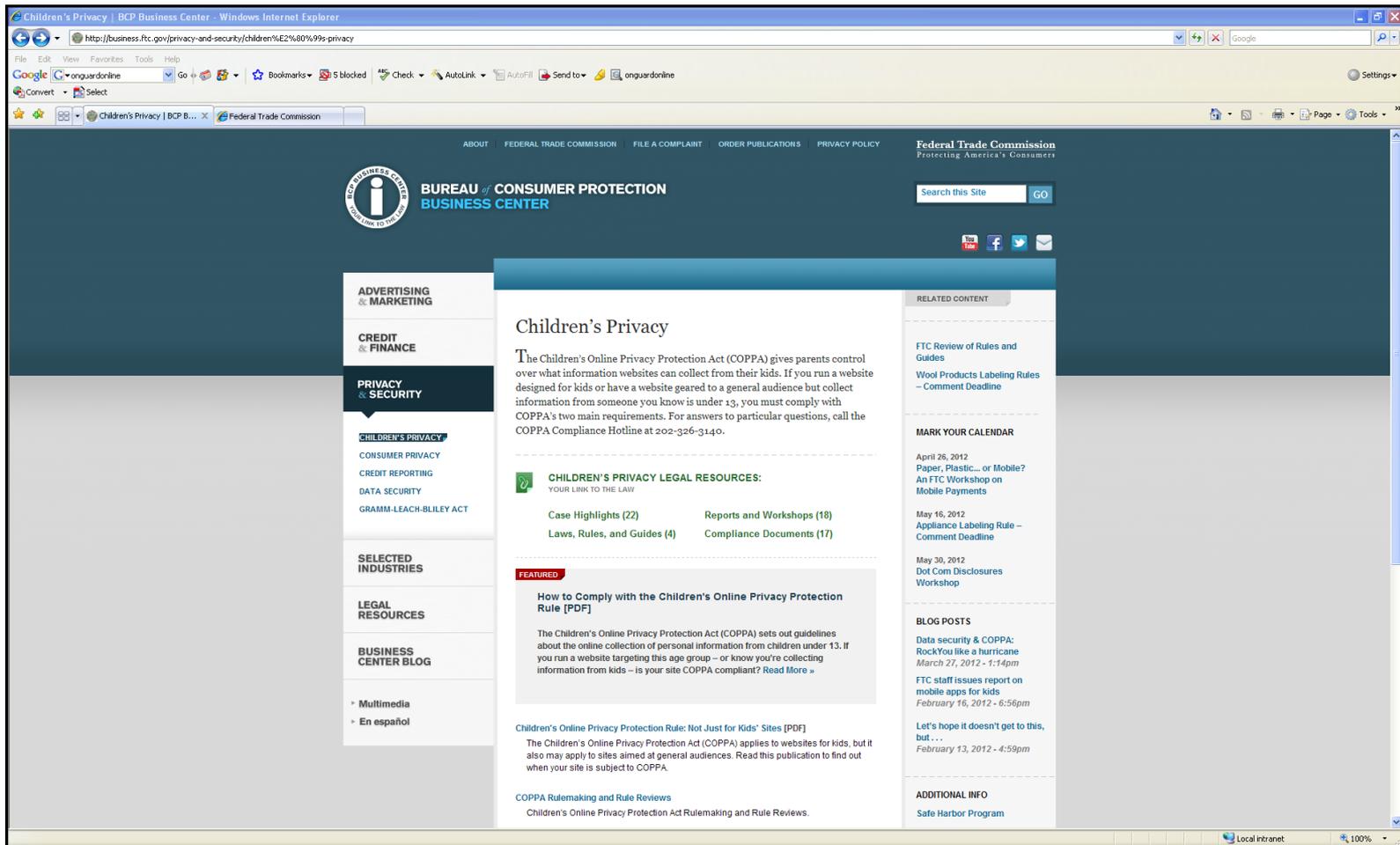
The screenshot shows the OnGuardOnline.gov website in a Windows Internet Explorer browser window. The browser's address bar displays the URL <http://onguardonline.gov/>. The website's header features the OnGuardOnline.gov logo, a search bar, and a language selector set to "Español". Below the header, a navigation menu includes links for "Avoid Scams", "Secure Your Computer", "Protect Kids Online", "Be Smart Online", "Video and Media", and "OnGuard Online Blog".

The main content area is divided into several sections:

- Blog:** A featured article titled "Mobile Devices Roundtable: Identifying Good Privacy and Security Practices" dated April 4, 2012, by Cora Tung Han, Attorney, Division of Privacy and Identity Protection, FTC. The article text begins: "Recently, I had the opportunity to speak at a Mobile Devices Roundtable organized by the HHS Office of the National Coordinator for Health IT (ONC) and the HHS Office for Civil Rights (OCR). The Roundtable was part of HHS' initiative to identify..." with a "Read More" link.
- Just for You...:** A list of targeted audience groups: Educators, Parents, Techies, Small Business, Military, and Kids.
- Learn more about the Net Cetera Outreach Toolkit:** A promotional graphic for a toolkit with navigation arrows.
- Avoid Scams:** A section with an icon of a laptop with a question mark and a list of links: "Phishing" and "Online Dating Scams". A "View more articles" link is at the bottom.
- Protect Kids Online:** A section with an icon of a person and a laptop and a list of links: "Cyberbullying" and "Kids and Socializing Online". A "View more articles" link is at the bottom.
- Be Smart Online:** A section with an icon of a laptop and a list of links: "Cookies: Leaving a Trail on the Web" and "Comparing Products Online". A "View more articles" link is at the bottom.
- Secure Your Computer:** A section with an icon of a laptop with a padlock and a list of links: "Securing Your Wireless Network" and "Malware". A "View more articles" link is at the bottom.
- Stay Connected:** A section with social media and newsletter options: "Get Email Updates", "Blog Feed", "Facebook", and "YouTube".
- Partner of the Day:** A section featuring the "Information Assurance Support Environment" logo and text: "Since 1998, the Information Assurance Support Environment (IASE) website has been identified as a 'one stop shop' for sharing IA..." with a "Read more" link. A "Learn about our Partners" link is also present.

The browser's status bar at the bottom indicates "Local intranet" and "100%" zoom.

Educating Businesses



The screenshot shows the BCP Business Center website in a Windows Internet Explorer browser window. The address bar displays the URL: <http://business.ftc.gov/privacy-and-security/children%E2%80%99s-privacy>. The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The toolbar shows various icons for navigation and utility. The website header features the Federal Trade Commission logo and the text "BUREAU of CONSUMER PROTECTION BUSINESS CENTER". A search bar is located in the top right corner. The main content area is titled "Children's Privacy" and includes a paragraph explaining the Children's Online Privacy Protection Act (COPPA). A sidebar on the left contains navigation links for Advertising & Marketing, Credit & Finance, Privacy & Security, and Selected Industries. A right sidebar contains related content, a calendar, and blog posts.

Children's Privacy

The Children's Online Privacy Protection Act (COPPA) gives parents control over what information websites can collect from their kids. If you run a website designed for kids or have a website geared to a general audience but collect information from someone you know is under 13, you must comply with COPPA's two main requirements. For answers to particular questions, call the COPPA Compliance Hotline at 202-326-3140.

CHILDREN'S PRIVACY LEGAL RESOURCES:
YOUR LINK TO THE LAW

- Case Highlights (22)
- Reports and Workshops (18)
- Laws, Rules, and Guides (4)
- Compliance Documents (17)

FEATURED

How to Comply with the Children's Online Privacy Protection Rule [PDF]

The Children's Online Privacy Protection Act (COPPA) sets out guidelines about the online collection of personal information from children under 13. If you run a website targeting this age group – or know you're collecting information from kids – is your site COPPA compliant? [Read More »](#)

Children's Online Privacy Protection Rule: Not Just for Kids' Sites [PDF]

The Children's Online Privacy Protection Act (COPPA) applies to websites for kids, but it also may apply to sites aimed at general audiences. Read this publication to find out when your site is subject to COPPA.

COPPA Rulemaking and Rule Reviews

Children's Online Privacy Protection Act Rulemaking and Rule Reviews.

RELATED CONTENT

- FTC Review of Rules and Guides
- Wool Products Labeling Rules – Comment Deadline

MARK YOUR CALENDAR

- April 26, 2012
Paper, Plastic... or Mobile?
An FTC Workshop on Mobile Payments
- May 16, 2012
Appliance Labeling Rule – Comment Deadline
- May 30, 2012
Dot Com Disclosures Workshop

BLOG POSTS

- Data security & COPPA: RockYou like a hurricane
March 27, 2012 - 1:14pm
- FTC staff issues report on mobile apps for kids
February 16, 2012 - 6:56pm
- Let's hope it doesn't get to this, but...
February 13, 2012 - 4:59pm

ADDITIONAL INFO

- Safe Harbor Program