



July 12, 2010

Hon. Donald S. Clark
Federal Trade Commission
Office of the Secretary, Room H-135 (Annex E)
600 Pennsylvania Avenue, NW
Washington, DC 20580

VIA ELECTRONIC FILING

Google Inc. is pleased to submit these comments in response to the Federal Trade Commission's [request](#) for comments on the Children's Online Privacy Protection Rule.

Founded in 1998, the same year in which the Children's Online Privacy Protection Act was passed by Congress, Google has been an active participant in the development of the Internet. Our company mission is to organize the world's information and make it universally accessible and useful. To this end, Google strives to provide users with valuable information and services through [Google Web Search](#), [Google News](#), [Gmail](#), [Google Maps](#), [YouTube](#), and a host of other new and emerging products. Google also recognizes the importance of user trust to the Internet's success and shares the Commission's commitment to ensuring that all persons, including children, enjoy appropriate privacy protections online.

In our recent [Privacy Roundtable comments](#), we gave the Commission an overview of our continuing efforts to increase the safety and privacy of all users online. In these comments, we describe more specifically the variety of tools and policies Google has implemented to protect children online, including robust enforcement mechanisms, innovative safety features, educational efforts aimed at users, and active partnerships with prominent organizations committed to online safety. We also address below some of the specific questions about COPPA and the FTC's rules raised in the request for comments.

Enhancing the Safety and Privacy of All Persons Online, Including Children

The Commission has [asked](#) how the COPPA rule has benefited children, parents, or other consumers. Additionally, the Commission has inquired into the impact that the COPPA rule has had on operators. Google is pleased to offer its perspective on these questions as an operator of general audience websites.

Google has taken a multi-pronged approach to enhancing the safety and privacy of all our online users. Although we restrict our services, we are still committed to protecting all users who are using Internet services and can benefit from educational tools and materials, including kids. At the outset, we note that we do not permit children younger than 13 to create Google accounts. Google accounts provide access and personalization across a variety of Google services. Users who [register](#) for Google accounts must provide their date

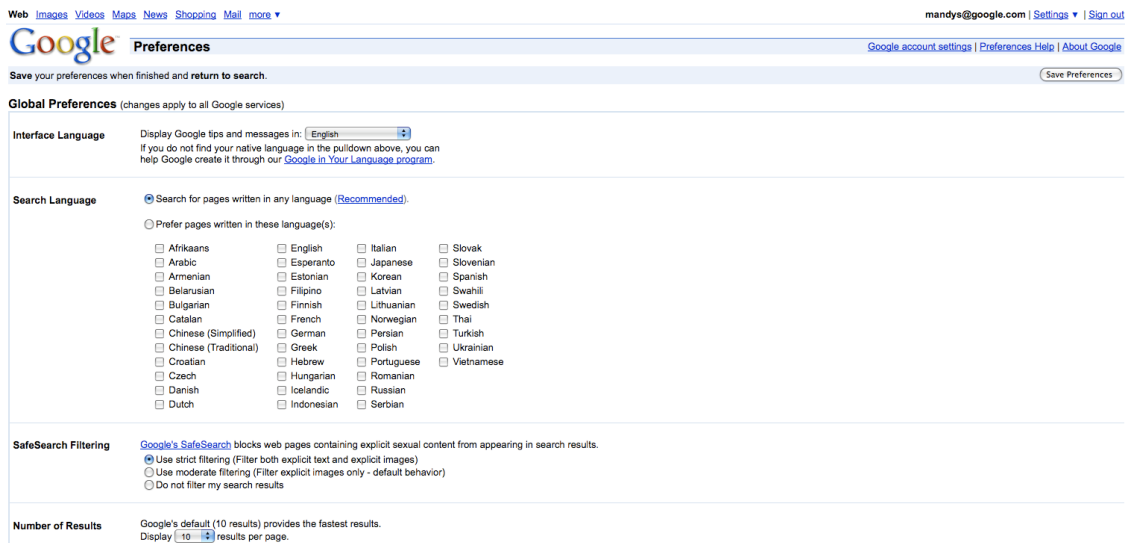
of birth and we screen to prevent children under 13 from obtaining accounts. If we subsequently gain actual knowledge that a Google account belongs to a user under 13, we remove the user's account in accordance with the Commission's COPPA rule guidance.

In addition to these precautions, Google takes an active role in promoting online safety and privacy through a combination of technical solutions, programs to combat illegal content and abuse, and educational initiatives. We describe some of our many offerings below.

Technical Tools

“SafeSearch Lock”

Google understands that many users prefer search results not to display adult sites or explicit content, particularly if children may use the same computer. Google has therefore developed a [SafeSearch](#) feature that parents may use to prevent their children from being exposed to sexually explicit images and text in search results.



The screenshot shows the Google Preferences page. At the top, there are navigation links for Web, Images, Videos, Maps, News, Shopping, Mail, and more. The user's email address (mandys@google.com) and a Sign out link are visible. The main heading is "Preferences" with links for Google account settings, Preferences Help, and About Google. Below this, there is a "Save your preferences when finished and return to search." button and a "Save Preferences" button.

Global Preferences (changes apply to all Google services)

Interface Language Display Google tips and messages in: . If you do not find your native language in the pulldown above, you can help Google create it through our [Google in Your Language program](#).

Search Language Search for pages written in any language (Recommended). Prefer pages written in these language(s):

| | | | |
|--|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> Afrikaans | <input type="checkbox"/> English | <input type="checkbox"/> Italian | <input type="checkbox"/> Slovak |
| <input type="checkbox"/> Arabic | <input type="checkbox"/> Esperanto | <input type="checkbox"/> Japanese | <input type="checkbox"/> Slovenian |
| <input type="checkbox"/> Armenian | <input type="checkbox"/> Estonian | <input type="checkbox"/> Korean | <input type="checkbox"/> Spanish |
| <input type="checkbox"/> Belarusian | <input type="checkbox"/> Filipino | <input type="checkbox"/> Latvian | <input type="checkbox"/> Swahili |
| <input type="checkbox"/> Bulgarian | <input type="checkbox"/> Finnish | <input type="checkbox"/> Lithuanian | <input type="checkbox"/> Swedish |
| <input type="checkbox"/> Catalan | <input type="checkbox"/> French | <input type="checkbox"/> Norwegian | <input type="checkbox"/> Thai |
| <input type="checkbox"/> Chinese (Simplified) | <input type="checkbox"/> German | <input type="checkbox"/> Persian | <input type="checkbox"/> Turkish |
| <input type="checkbox"/> Chinese (Traditional) | <input type="checkbox"/> Greek | <input type="checkbox"/> Polish | <input type="checkbox"/> Ukrainian |
| <input type="checkbox"/> Croatian | <input type="checkbox"/> Hebrew | <input type="checkbox"/> Portuguese | <input type="checkbox"/> Vietnamese |
| <input type="checkbox"/> Czech | <input type="checkbox"/> Hungarian | <input type="checkbox"/> Romanian | |
| <input type="checkbox"/> Danish | <input type="checkbox"/> Icelandic | <input type="checkbox"/> Russian | |
| <input type="checkbox"/> Dutch | <input type="checkbox"/> Indonesian | <input type="checkbox"/> Serbian | |

SafeSearch Filtering [Google's SafeSearch](#) blocks web pages containing explicit sexual content from appearing in search results.

Use strict filtering (Filter both explicit text and explicit images)

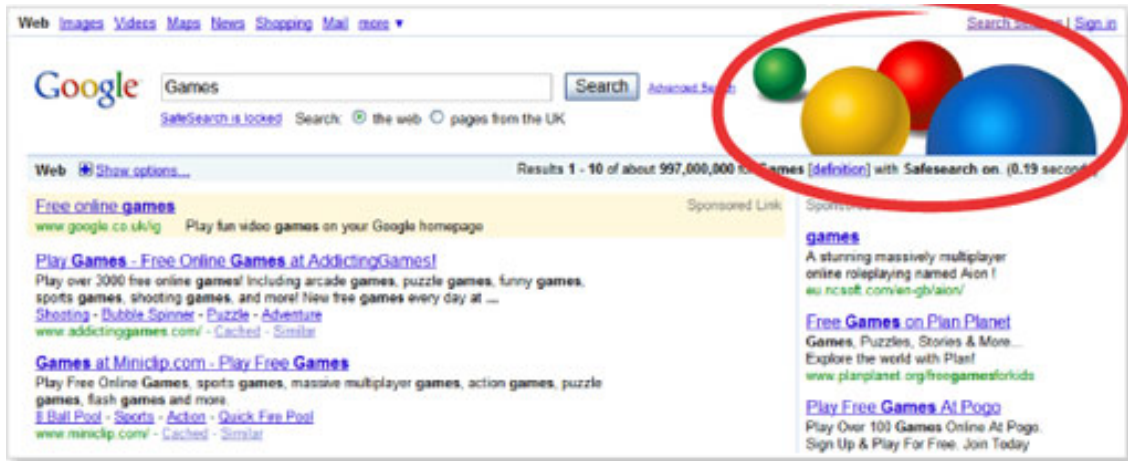
Use moderate filtering (Filter explicit images only - default behavior)

Do not filter my search results

Number of Results Google's default (10 results) provides the fastest results. Display results per page.

Setting Safe Search preference

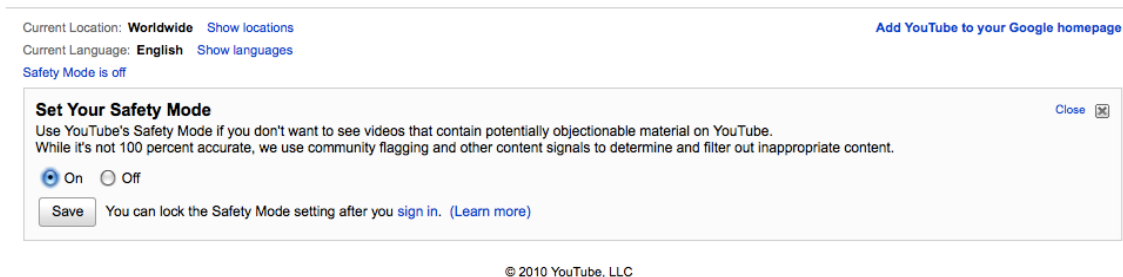
Google [recently](#) enhanced the SafeSearch feature by adding the SafeSearch Lock option, which allows users, such as parents, to lock their SafeSearch setting to the strict screening level. Once the SafeSearch screen level has been set, the level cannot be changed without a password. Parents can [observe](#) whether the feature is on, even from across a room, because the feature displays colored balls across the top of the monitor screen when the setting is locked.



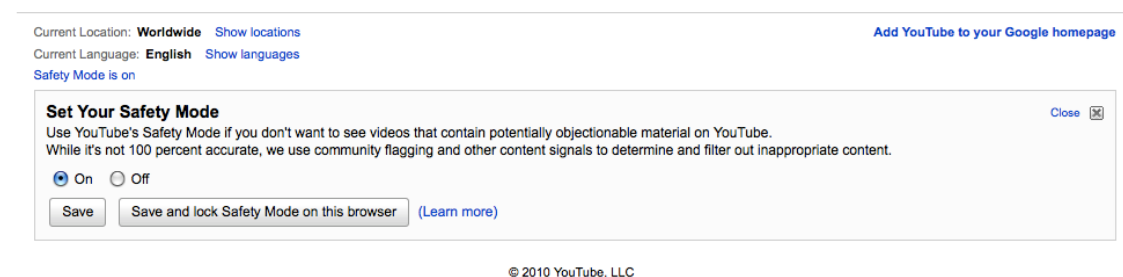
SafeSearch when locked

"YouTube Safety Mode"

On YouTube, a video sharing website owned by Google, users may exercise control over their experiences by choosing the Safety Mode setting. The Safety Mode setting was [launched](#) and designed to prevent users or their children from being exposed to content that they prefer not to see.



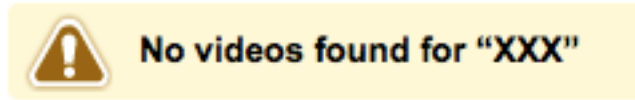
Safety Mode: not signed in



Safety Mode: signed in

If users select Safety Mode, the feature prevents videos with potentially objectionable

content and videos that have been restricted to users 18 and older from displaying in video search, related videos, playlists, shows, and movies.

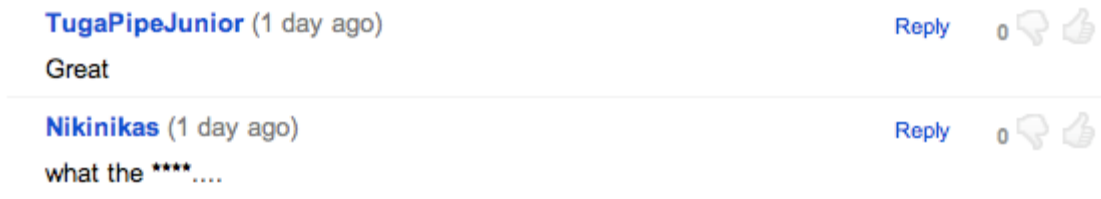


Safety Mode video search

Parents may select this Safety Mode by clicking on the link at the bottom of any video page. Additionally, they may lock the setting on the browser with a YouTube password.

“Hide Objectionable Words” Option in YouTube

Google provides a Hide Objectionable Words option for YouTube. This feature helps block profanity, sexually suggestive language, and racial slurs. Users may also replace commentary that they find to be age-inappropriate with asterisks in user comments.

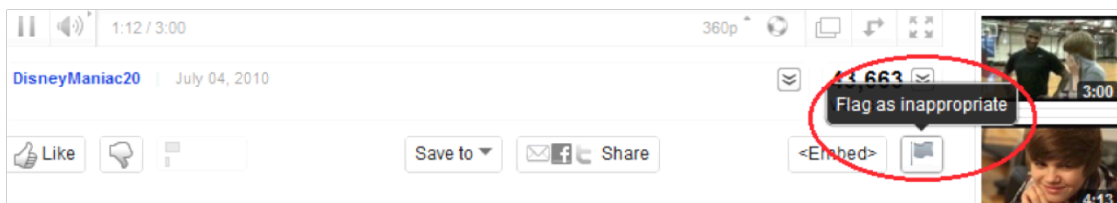


Hide objectionable words

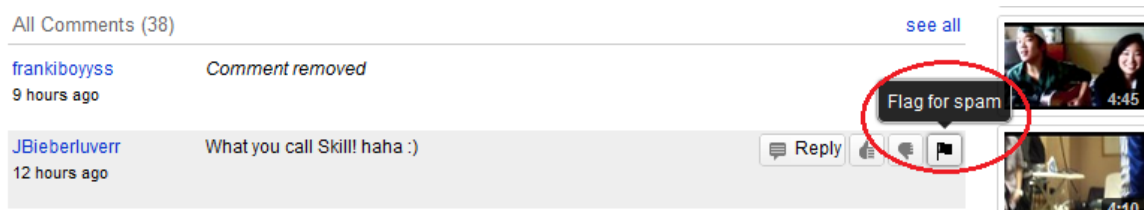
Users may easily activate this feature by clicking on “Options” next to the Comments header and checking the “Hide Objectionable Words” box. YouTube users can also hide comments completely by clicking “Hide Comments.” These [selections remain in effect](#) until users change their preferences.

Flagging Content and Reporting Spam in YouTube

Users can [flag](#) inappropriate videos that violate Google’s Terms of Use and/or YouTube Community Guidelines and [report](#) comments appearing underneath videos as spam. These tools empower users as a community to regulate and control the content that is available to be viewed by children as well as other users.



Flagging videos for objectionable content



Reporting comments as spam

Cooperation with Industry Partners, Community Stakeholders, and Law Enforcement

Google builds and maintains strong relationships with industry partners, community stakeholders, and law enforcement to improve users' online experiences and to combat illegal activity. For example, Google is a proud member of the PointSmart ClickSafe Task Force that focuses on Internet safety in the United States. This Task Force, which is comprised of technology companies, child advocacy and parents' groups, educators, researchers, and policymakers, recently [released](#) its "Recommendations for Best Practices for Online Safety and Literacy." The report highlighted the need for digital media literacy and online safety education among children, parents, and educators to enable them to think critically about content creation and other online activities.

Google has provided funding to and worked with a number of partners that share and advance Google's commitment to online safety, including Family Online Safety Institute, Common Sense Media, Connect Safely, and iKeepSafe. Among other things, we hold discussions with some of our partners to solicit feedback and guidance on our efforts to promote children's online safety. Google has also worked with many of these organizations to educate parents, teachers, and communities about how to help children learn responsible online behaviors and best practices.

Google also actively cooperates with law enforcement and other partners to combat child sexual abuse. When we become aware of child sexual abuse images or child pornography in our search engine results or hosted on our sites, we immediately remove them and report the incidents to law enforcement through the National Center for Missing and Exploited Children. With NCMEC, we also work with engineers to develop new technical solutions aimed at eradicating online child pornography and identifying and locating exploited children. Since a child must be identified before a warrant for arrest can be issued, we have recently worked with NCMEC to identify how to accelerate internal processes to expedite investigations. In recent years, Google has made significant donations of hardware and software to help improve NCMEC's data management capabilities. For instance, we recently awarded an additional \$1 million grant to NCMEC to support its important mission.

Educational Initiatives

Google engages in a variety of educational initiatives to promote adoption of our safety tools and to educate families about how to use the Internet responsibly. We recently launched a

Family Digital Literacy Tour. As part of this initiative, we have been traveling across the country promoting an in-class curriculum that we developed with iKeepSafe that teaches middle school children how to recognize online risks, investigate and determine the reliability of websites, and avoid scams. To complement our efforts in the classroom, we are training parents, teachers, and volunteers to host future workshops and providing advice on how to talk to children about best practices for going online.

Additionally, Google maintains blog posts, safety guides, and readily-accessible help pages, such as YouTube's Safety Center, to provide parents and youth with tips about [staying safe online](#). These resources include a series of digital citizenship and online safety videos, including [clips](#) on "Playing and Staying Safe Online," "Detecting Lies and Staying True," "Staying Safe on YouTube," and "Steering Clear of Cyber Tricks." Google has also used its platforms to highlight resources offered by others, such as the FTC, in furtherance of Internet safety. For instance, Google's Public Policy Blog recently featured a posting on the Commission's interactive game called [Admongo](#), where children can learn about ads and commercial messages.

"Personal Information" Should Include Information That Reasonably Identifies an Individual

The Commission has inquired about expanding the COPPA rule to apply to additional types of information. Specifically, the Commission [requested comment](#) on the possibility of expanding the definition of the term "personal information" to include information collected with online behavioral advertising, persistent IP addresses, mobile geolocation information, screen names, passwords, zip codes, dates of birth, and gender.

Information should not constitute "personal information" unless it is information about a specific individual and is used to identify the individual. For example, zip codes by themselves do not personally identify an individual and thus should not be captured under the definition of "personal information." Including such information within the scope of the term could complicate the ability of companies to provide useful services that rely on the collection of zip code information for such functions as determining appropriate time zones and geographical locations. The other categories of information discussed in the Commission's request for comments, including information collected for advertising purposes, likewise do not inherently identify an individual but are used to enhance consumers' online experiences. These types of information should not constitute "personal information" unless a provider is actually combining the information with data that identifies a specific person.

Similarly, persistent IP addresses should not be included as a category of "personal information" because IP addresses do not inherently identify individuals and do not permit the types of "contact" that COPPA was intended to address. To begin with, IP addresses pertain to a specific computer or device, not an individual. For instance, during the course of an evening, multiple patrons might conduct Google searches from a computer at a public library; based on an examination of the IP address, Google would have no means of knowing whether a child or adult is conducting the search. Google would also have no means of knowing whether an individual who conducted a Google search from one

computer was the same person who later conducted a search from another computer using a different IP address.

Moreover, including IP addresses within the definition of “personal information” would be operationally challenging and technically impractical within the COPPA framework without corresponding benefit to child safety and privacy. As discussed above, many individuals could use the same computer or a single person could use multiple devices associated with different IP addresses. An operator therefore would have no means of knowing who is conducting a search without forcing all users to sign in with a user name and password every time the users conducts a search. Such a requirement would lead to the perverse situation where an operator would be required to obtain and retain more personal information from individuals than would otherwise be necessary if IP addresses were not categorized as personal information.

Additionally, it is unclear how an operator could practically obtain consent before logging an IP address. In order to deliver a webpage to a viewer, an IP address must first be obtained in order to know where to deliver the page. Such information is currently collected automatically and it would not be feasible to attempt to ascertain a user’s age or to seek verifiable parental consent before obtaining the IP address. Thus, we believe that expanding “personal information” to cover persistent IP addresses would be unworkable.

The COPPA Rule Provides a Flexible Means of Obtaining Verifiable Parental Consent

The Commission has [asked](#) for feedback on Section 312.5(b)(2) of the COPPA rule, which provides a non-exhaustive list of approved methods of obtaining parental consent. Google supports retaining the [list](#) of approved methods of obtaining verifiable consent, including using credit cards in connection with a transaction. As written, the COPPA rule already provides operators with sufficient flexibility to develop innovative ways to obtain verifiable consent through technologies that are “reasonably calculated” to ensure that a person providing consent is the child’s parent. We encourage the Commission to retain this flexibility to allow the COPPA rule to encompass new means of obtaining parental consent as technologies evolve.

* * *

We thank you for the opportunity to provide comments on this important subject. Please do not hesitate to contact me with any questions by email at pablochavez@google.com or by phone at 202.346.1237.

Sincerely,

Pablo L. Chavez
Director of Public Policy
Google Inc.