Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 1, 2014

M. Nottingham

May 30, 2014

# The "safe" HTTP Preference
# draft-nottingham-safe-hint-02

## Abstract

This specification defines a "safe" preference for HTTP, expressing a user preference to avoid "objectionable" content.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 1, 2014.

## Copyright Notice

Table of Contents

1. Introduction . . . . . 2
1.1. Notational Conventions . . . . . 3
2. The "safe" Preference . . . . . 3
3. Security Considerations . . . . . 4
4. IANA Considerations . . . . . 4
5. References . . . . . 5
5.1. Normative References . . . . . 5
5.2. Informative References . . . . . 5
Appendix A. Acknowledgements . . . . . 6
Appendix B. Setting "safe" from Web Browsers . . . . . 6
Appendix C. Using "safe" on Your Web Site . . . . . 6

## 1. Introduction

Many Web sites have a "safe" mode, to assist those who don't want to be exposed (or have their children exposed) to "objectionable" content. YouTube [youtube], Yahoo! Search [yahoo], Google Search [google], Bing Search [bing], and many other services have such a setting.

However, those who wish to have this preference honoured need to go to each Web site in turn, navigate to the appropriate page, (possibly creating an account along the way) to get a cookie [RFC6265] set in the browser. They would need to do this for each browser on every device they use.

This is onerous to achieve effectively, because there are so many permutations of sites, user agents and devices.

If this preference is proactively advertised by the user agent, things become much simpler. A user agent that supports doing so (whether it be an individual browser, or through an Operating System HTTP library) need only be configured once to assure that the preference is advertised to all sites that understand and choose to act upon it. It's no longer necessary to go to each site that has potentially "unsafe" content and configure a "safe" mode.

Furthermore, a proxy (for example, at a school) can be used to ensure that the preference is associated with all (unencrypted) requests flowing through it, helping to assure that clients behind it are not exposed to "objectionable" content.

This specification defines how to associate this preference with a request, as a HTTP Preference [I-D.snell-http-prefer].





Note that this approach does not define what "safe" is; rather, it is interpreted within the scope of each Web site that chooses to act upon this information (or not). As such, it does not require agreement upon what "safe" is, nor does it require application of policy in the user agent or an intermediary (which can be problematic for many reasons).

## 1.1. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

## 2. The "safe" Preference

When present in a request, the "safe" preference indicates that the user prefers content which is not objectionable, according to the server's definition of the concept.

For example, a request that includes the "safe" preference:

```
GET /foo.html HTTP/1.1
Host: www.example.org
User-Agent: ExampleBrowser/1.0
Prefer: safe
```

When configured to do so, user agents SHOULD include the "safe" preference in every request, to ensure that the preference is applied (where possible) to all resources.

For example, a Web browser might have a "Request Safe Browsing" option.

Additionally, other clients MAY insert it; e.g., an operating system might choose to insert the preference in requests based upon system-wide configuration, or a proxy might do so based upon its

configuration.

Origin servers that utilize the "safe" preference SHOULD document that they do so, along with the criteria that they use to denote objectionable content. If a server has more fine-grained degrees of "safety", it SHOULD select a reasonable default to use, and document that; it MAY use additional mechanisms (e.g., cookies) to fine-tune.

A response corresponding to the request above might have headers that look like this:





```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Content-Type: text/html
Server: ExampleServer/2.0
Vary: Prefer
```

Note that the Vary response header needs to be sent if cacheable responses associated with the resource might change depending on the value of the "Prefer" header. This is not only true for those responses that are "safe", but also the default "unsafe" response.

See [I-D.ietf-httpbis-p6-cache] for more information.

## 3. Security Considerations

The "safe" preference is not a secure mechanism; it can be inserted or removed by intermediaries with access to the data stream. Its presence reveals information about the user, which may be of small assistance in "fingerprinting" the user (1 bit of information, to be precise).

Due to its nature, including "safe" in requests does not assure that all content will actually be safe; it is only when servers elect to honour it that content might be "safe".

Even then, a malicious server might adapt content so that it is even less "safe" (by some definition of the word). As such, this mechanism on its own is not enough to assure that only "safe" content is seen; users who wish to ensure that will need to combine its use

with other techniques (e.g., content filtering).

Furthermore, the server and user may have differing ideas regarding the semantics of "safe." As such, the "safety" of the user's experience when browsing from site to site might (and probably will) change.

## 4. IANA Considerations

This specification registers the "safe" preference [I-D.snell-http-prefer]:

- Preference: safe
- Value: (no value)
- Description: Indicates that the user (or one responsible for them) prefers "safe" or "unobjectionable" content.





- Reference: (this document)
- Notes:

## 5. References

### 5.1. Normative References

[I-D.snell-http-prefer] Snell, J., "Prefer Header for HTTP", draft-snell-http-prefer-18 (work in progress), January 2013.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

### 5.2. Informative References

[I-D.ietf-httpbis-p6-cache] Fielding, R., Nottingham, M., and J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Caching", draft-ietf-httpbis-p6-cache-26 (work in progress), February 2014.

[RFC6265] Barth, A., "HTTP State Management Mechanism", RFC 6265, April 2011.

[bing] Microsoft, "Bing Help: Block Explicit Web Sites", 2013, <http://onlinehelp.microsoft.com/en-AU/bing/ff808441.aspx>.

[google] Google, "SafeSearch: turn on or off", 2013, <http://support.google.com/websearch/bin/answer.py?p=settings_safesearch&answer=510>.

[yahoo] Yahoo! Inc., "Yahoo! Search Preferences", 2013, <http://search.yahoo.com/preferences/preferences>.

[youtube] Google, "How to access and turn on Safety Mode?", 2013, <http://support.google.com/youtube/bin/answer.py?answer=174084>.





## Appendix A. Acknowledgements

Thanks to Alissa Cooper, Ilya Grigorik, Emma Llanso, Jeff Hughes and Loorie Cranor for their comments.

## Appendix B. Setting "safe" from Web Browsers

As discussed in Section 2, there are many possible ways for the "safe" preference to be generated. One possibility is for a Web browser to allow its users to configure the preference to be sent.

When doing so, it is important not to misrepresent the preference as binding to Web sites. For example, an appropriate setting might be a checkbox with wording such as:

[] Request "safe" content from Web sites

... along with further information available upon request (e.g., from a "help" system).

Browsers might also allow the "safe" preference to be "locked" - that is, prevent modification without administrative access, or a passcode.

## Appendix C. Using "safe" on Your Web Site

Web sites that allow configuration of a "safe" mode (for example, using a cookie) can add support for the "safe" preference incrementally; since the preference will not be supported by all clients immediately, it is necessary to still have a fallback configuration option.

When honouring the safe preference, it is important that it not be possible to disable it through the Web interface, since "safe" may be inserted by an intermediary (e.g., at a school) or configured and locked down by an administrator (e.g., a parent). When both the "safe" preference and per-site configuration are present, the preference takes precedence.

The safe preference is designed to make as much of the Web a "safe" experience as possible; it is not intended to be configured site-by-site. Therefore, if the user expresses a wish to disable "safe" mode, the site should remind them that the safe preference is being sent, and ask them to consult their administrator (since "safe" might be set by an intermediary or locked-down Operating System configuration).





As explained in Section 2, responses that change based upon the presence of the "safe" preference need to either carry the "Vary: Prefer" response header field, or be uncacheable by shared caches (e.g., with a "Cache-Control: private" response header field). This is to avoid an unsafe cached response being served to a client that prefers safe content (or vice versa).

## Author's Address

Mark Nottingham

EMail: mnot@mnot.net
URI: http://www.mnot.net/