Human Rights Protocol Considerations Research Group
Internet-Draft
Intended status: Informational
Expires: January 16, 2018

S. Abraham
CIS India
MP. Canales
Derechos Digitales
O. Khrustaleva
American University
C. Runnegar
ISOC

July 15, 2017

Human Rights Considerations for RFC7725
draft-manyfolks-hrcrfc7725-00

Abstract

This is draft applies the model for developing human rights protocol considerations as defined in draft-irtf-hrpc-research for [RFC7725].

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 January 16, 2018.

Copyright Notice

Table of Contents

1. Introduction

This is draft applies the model for developing human rights protocol considerations as defined in draft-irtf-hrpc-research for RFC7725.

2. Connectivity

HTTP 451 status code response can be sent by the end nodes as well as by intermediary nodes, which makes for a potential anonymity breach possible. However, this anonymity breach needs to be intentional.

3. Visibility in a browser

In the web-browsing context, the HTTP status code response might only be issued for a sub-resource (e.g. images, videos, extra HTML, CSS, or JavaScript, which are each fetched using separate requests),

rather than the top-level resource seen in a browser's address bar. For example, consider a web page at https://example.net/video/ with an embedded video window implemented in html as

<video><source src="movie.webm"><video>.

https://example.net/video/ may return HTTP 200, but https://example.net/video/movie.webm may return HTTP 451. Multiple subresources on a given page may return 451.

This means that visibility to a browser user might be more complex than just "this web page has been blocked".

4. Privacy

A HTTP 451 status code response could be visible to an observer on the network. An observer may be able to discern the blocked domain or URL the user attempted to access. Therefore, implementers should deploy HTTP status code over HTTPS to mitigate this privacy risk. See also RFC 7540 Hypertext Transfer Protocol Version 2 (HTTP/2), section 10.8 privacy considerations. Even where HTTPS is used, metadata is still available to an observer. That metadata could be used to identify a device, it's location and/or a user (especially when combined with other observable data).

Some implementations of [RFC7725] send the HTTP status code response and then re-direct to another URL [insert reference to research revealing this]. [also describe the specific redirection mechanism(s) used - javascript? html meta refresh tag? something else?] [insert text as to why this is a problem from a privacy perspective]. Implementers should not imbed tracking elements in either web resource.

[RFC7725] provides that a HTTP status code 451 is cachable by default. Caching status code 451 on users' devices means that there will be a record of their attempt to access the blocked content stored on their devices. If caching is used, the 451 status code response should notify users.

HTTP 451 status code responses are unverified and may be fake and/or a vehicle to monitor the user and/or introduce malware.

5. Content Agnosticism

There may be an issue of content agnosticism if the resource returning the HTTP 451 status code is only blocked for some users (e.g. geo-blocking). This is not a protocol issue, but rather an artefact of the blocking order. The status code 451 is both content

agnostic and content gnostic. It is content agnostic from the perspective of the end-user when the blocking is done at the level of the resource. However, when blocking is done at the level of the sub-resource it may not be content agnostic in all cases from the perspective of the end user. If the sub-resource is HTML then the end user will be able to see the details of the block beyond just the status code. But if the sub-resource is an image, audio or video - the browser will not be able to render the details of the block since the browsers currently will not render the information from the header in a manner that is scrutable to the end user. This concern could be partially addressed by using an appropriate plugin that is able to parse the header.

6. Security

HTTP 451 status code responses are unverified which make them a possible vehicle to introduce malware. The malware could be specifically implemented with the purpose to surveil the final user that is trying to access an specific type of content that has been censored.

7. Internationalization

The RFC does not require the use of any particular language and therefore when the standard is being implemented any language could be used.

8. Censorship Resistance

While HTTP 451 status code cannot prevent censorship it can help make censorship more transparent and make assessment of Internet censorship cases easier. "Censorship is where an entity in a position of power - such as a government, organization, or individual - suppresses communication that it considers objectionable, harmful, sensitive, politically incorrect or inconvenient." Legal means have been used for censoring content for a long time, and what HTTP 451 status code does is demonstrate when legal means meet technical means online. Blocking is still censorship, and status code 451 doesn't solve the problem, but creates a way for more transparent reporting of censorship that can be useful for the analysis and advocacy. Also, If the users are informed about why their access to a specific resource was denied they can opt to use circumvention techniques.

9. Open Standards

RFC 7725 is an open standard.

10. Heterogeneity Support

A HTTP 451 status code response can be used for any HTTP or HTTPS web resource and for any software, applications and devices that are capable of displaying HTTP header responses.

11. Anonymity

Possible anonymity concerns as identifiers might be introduced by the parties serving 451 status code.

12. Accessibility

The RFC can be currently implemented in two ways for resources. Either the server could either return a HTML file without any automatic redirect or a HTML file with an automatic redirect. The second option could interfere with accessibility because disabled end users may not have sufficient time to use their accessibility software and hardware to read the status code and other details. Therefore it is recommended that the RFC be updated to ensure that the display of a HTTP 451 status code response should be untimed and static to provide users enough time to read and use the content.

13. Localization

HTTP 451 status code implies a reference to legal reasons for making a content unaccessible. Those legal implications usually will concern a national legal framework that it will not be always easy to understand for non legal operators or users from different jurisdictions who are being affected by the lack of access for legal reasons. When it comes to localization for language, locale etc. the RFC does not explicitly provide for internationalization of text strings but implementers of the standards can localize the text strings nevertheless.

14. Reliability

HTTP 451 status code responses are unverified so they could be fake or mistaken. The protocol by itself does not prevent the misuse of the status code or wrong tagging of other unavailability reasons. The informational requirement as part of the protocol address this concern in some extent, but commonly it will be difficult for the end user to verify if the code has been correctly used or if the information provided as part of it is truthful. Additionally, many companies include in their Terms of Service prohibited types of content or activities on their networks, reserving to their discretion the interpretation of broad terms used to capture many forms of content that can be potentially blocked.

15. Confidentiality

HTTP 451 status code use implies sharing of information by the reporter that make it easier to identify where censorship is taking place. It can expose to governments engaging with censorship who is more willing to collaborate blocking content making them an easier target for further actions of censorship.

16. Integrity

For integrity, a status code 451 should be delivered over HTTPS.

17. Authenticity

Implementation of the status code 451 could guarantee authenticity in most cases if the server operators implement HTTPS. However that only guarantees authenticity during the last mile of transit between the server serving the status code and the end user. There is no way in which the status code guarantee that the server operator is not serving false information about a particular instance of censorship. This could happen deliberately under a variety of circumstance - the server operator is masking self-censorship as government censorship or the server operator has self-interest in misrepresenting the facts about government or private censorship. Lack of legal expertise or capacity could also result in false information being served to the user. Many start-ups and non-profits cannot afford legal teams with the requisite expertise and many large corporation reserve their best lawyers for core business activities leaving censorship related activities to interns and junior staff. There is no real incentive beyond good (corporate) citizenship for server operators to tell the truth and therefore this is an area for concern when it comes to implementation of the status code.

18. Adaptability

Status code 451 does not have any legal or technical limitations which prevents the development of other standards / protocols.

19. Outcome Transparency

The assumption behind the development of the status code 451 is that transparency has a chilling effect on censorship and that transparency will enable the process of justice by allowing acts of censorship to be challenged. This is the very same assumption behind the publication of transparency reports by various Internet corporations like Google, Facebook and Twitter. Unfortunately, this has not always been the case - in some countries the transparency reports may have contributed to competitive behavior thereby

increasing censorship. In some countries, blocks orders are unevenly implemented by ISPs either because it does not serve their bottom-lines or they are resisting censorship - governments in those countries could mandate the implementation of status code 521 which will make it easier for them to monitor the implementation of their block orders. Finally, surveillance systems in some countries could be updated to watch out for the 521 error code on unencrypted traffic making it easier to identify those trying to access prohibited content. Before the implementation of this standard there would be no uniformity in which websites would implement a block order increasing the number of false positives for any automated monitoring systems.

20. Security Considerations

As this document concerns a research document, there are no security considerations.

21. IANA Considerations

This document has no actions for IANA.

22. Research Group Information

The discussion list for the IRTF Human Rights Protocol Considerations Research Group is located at the e-mail address hrpc@ietf.org [1]. Information on the group and information on how to subscribe to the list is at https://www.irtf.org/mailman/listinfo/hrpc

Archives of the list can be found at: https://www.irtf.org/mail-archive/web/hrpc/current/index.html

23. References

23.1. Informative References

[RFC7725] Bray, T., "An HTTP Status Code to Report Legal Obstacles", RFC 7725, DOI 10.17487/RFC7725, February 2016, <http://www.rfc-editor.org/info/rfc7725>.

23.2. URIs

[1] mailto:hrpc@ietf.org

Authors' Addresses

Sunil Abraham
CIS India

EMail: sunil@cis-india.org

Maria Paz Canales
Derechos Digitales

EMail: mariapaz@derechosdigitales.org

Olga Khrustaleva
American University

EMail: ok4193a@student.american.edu

Christine Runnegar
ISOC

EMail: runnegar@isoc.org