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

S. Abraham
CIS India
MP. Canales
Derechos Digitales
J. Hall
CDT
O. Khrustaleva
American University
N. ten Oever
ARTICLE 19
C. Runnegar
ISOC
S. Sahib
Cisco Systems
July 15, 2017

# Implementation Report for HTTP Status Code 451 (RFC 7725) draft-451-imp-report-00

## Abstract

This report describes implementation experience between various components working with the HTTP Status Code 451 [RFC7725], a risk assessment and recommendation for improvements.

## 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 document evaluates the usage of HTTP Status Code 451, which was standardized by the IETF in February 2016 [RFC7725]. This implementation report aims to illuminate whether the status code does what it set out to do ("provide transparency in circumstances where issues of law or public policy affect server operations"), the different ways it is being used, positive and negative impacts the standard might have and we end with suggestions for improvement of the standard.

## 2. Vocabulary

Blocking The act of making an HTTP resource inaccessible to a class of users.

Resource A top-level information object served by an HTTP server (e.g., HTML page).

Subresource An information object served within the context of a top-level Resource (e.g., JavaScript, Image, etc.)

Server Operator An entity or an individual operating an HTTP server.

HTTP status For each response, HTTP servers return a numerical status code (e.g., 400 (OK), 403 (unauthorized), etc.) described by IANA https://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml.

Response When an HTTP Server responds to a request, it sends a Response, made up of header fields and a body (See: https://tools.ietf.org/html/rfc7725#section-3

Legal demand A verbal or written request grounded in law or regulation from an Authority to a Server Operator to Blocking a Resource.

Authority A government or government-licensed entity mandating blocking of a resource directly or that may institute laws that indirectly require blocking of a resource.

Complainant A party making a Legal demand; may or may not be an Authority (e.g., the US DMCA allows a copyright holder to demand takedown).

## 3. Target audiences

## 4. Who is likely to implement the 451 status code?

### 4.1. Server operators

Server operators that are being confronted with an order from a legal authority can use the HTTP Status Code to communicate to third parties why the resource is not available on the server.

### 4.2. Intermediaries

Intermediaries such as Internet Service Providers, Content Distribution Networks and other might be obligated by a legal authority in their operational jurisdiction to filter certain content. The HTTP status code would add transparency to this practice.

## 5. Who is likely to use the 451 status code data?

### 5.1. Browser vendors

Browser vendors might implement functionality to communicate the presence of a HTTP status code 451 to a user.

### 5.2. End users

End users will be informed about why the information they are trying to access is not available, instead of merely concluding that the content is not available due to other reasons (e.g., 404 unavailable).

### 5.3. Researchers

Researchers might want to scan for the prevalence of blocking, as well as trends in blocking behavior.

### 5.4. Civil society

Civil society may want to use instances of HTTP status code 451 to highlight censorship and censorship trends, to challenge blocking.

### 5.5. Governments

Governments might want to verify compliance with blocking orders and use HTTP status code 451 to do so on the networks in their jurisdiction.

## 6. Current Usage

## 7. Overview

In the majority of cases in which HTTP status code 451 is being deployed [Censys], the status code reads as follows - "451 Unavailable For Legal Reasons" or "451" or "451 Unknown Error" or "451 Error" or "451 Unavailable For Legal Reasons (burned)" or "451 OK". The Page Title could say "404 Not Found" or "Blocked" or "451 -" or "Restricted access" or "Bloqueado por ordem judicial" ("Blocked by judicial order") or "Sito censurato" ("Censored site") or "Доступ ограничен" ("Access is restricted") or "Зелёная точка - доступ к запрашиваемому ресурсу ограничен" ("Zelenaya tochka" - Internet and TV provider - access to the requested resource is restricted")or "Violazione del bispensiero" or "Please report sexual abuse against children to the Swedish National Bureau of Investigation!" or "Copyright Notice" or "451 RKN Redirect" (RKN is likely Russia's Roskomnadzor) or "ATTENZIONE!! - POLIZIA POSTALE E DELLE COMUNICAZIONI - PAGINA BLOCCATA" ("Attention! - Postal and Communications Policy - Blocked Page") or "451 Unavailable For Legal Reasons 本网站由于国家政策而不可用" (Chinese: "This site is not available due to national policy").

The hosts that were observed implementing the status code are located in Russia, United States of America, Singapore, Czech Republic, Thailand, Netherlands, Portugal, Spain, Italy, Greece, Bulgaria, Hungary, Germany, France, United Kingdom, Ukraine, Norway, Finland, Kazakhstan, United Arab Emirates, Japan, China, Philippines and Australia. In some cases - the visitor to the website is provided some context for the block - for example, a take-down notice for copyright infringment - in other cases the visitor is encouraged to cooperate with law enforcement agencies. The page title may have information that does not always make sense in the context of the error code, for example when the title says "404 Not Found" but the page is a 451 response body. These observations are based an examination of the search results from Censys.io on 15 July 2017 which featured 526 IPv4 Hosts of which 17 were included in the list of "Top Million Websites".

Several large content providers are now supporting the HTTP 451 Status Code, such as [Github] and [Reddit], whereas other content providers such as [Twitter], [Facebook], and [Youtube] are currently not using the HTTP status code to indicate the blocking or takedown of specific content.

## 8. Trends and observations

- The majority of instance of HTTP status code 451 provide no explanation in the response body.

- There have been found several cases of servers serving HTTP status code 451 with redirect another server with a central warning message of a blocking authority.

- A registrar serves HTTP status code 451 when a registrant did not pay their domain fees.

- There are significant observations of server serving HTTP status code 451 based on geoIP (especially for gambling sites).

- There are different understandings of the 'blocked-by' field as defined in RFC7725. Some people interpret is as the entity that is doing the blocking, others are interpreting it at the authority responsible for ordering the blocking.

- HTTP Status Code 451 is thusfar only served by hosts, not by intermediaries.

## 9. Potential negative or positive impacts

- [RFC7725] specifies a status code for web resources that are blocked for legal reasons. The HTTP status code 451 is designed to enable content providers and intermediaries (including ISPs and search engines) to notify users that their access to specific web resources has been blocked for legal reasons. The standard also recommends that the notification include an explanation. This is important because this is the detail the user needs to be able to understand why access has been blocked, and if desired, to take action to challenge the blocked access. It also helps content servers and intermediaries who have been required to block access to notify users who directed that access by blocked.

- Also, as the 451 status code is machine-readable, researchers and others could use web crawlers to identity which blocked URLs or sub-resources use error code 451. This data could be used to produce a searchable open repository of all known error code 451 instances. This information could then be used to map the blocked

Web and to analyze the explanations, looking for trends and anomalies. For example, one day there might be an answer to the question - "how much content is blocked for IPR reasons?"

- The 451 status code can also be used for encrypted webpages, which is significant as encryption on the Web becomes more and more prevalent. A user should be able to see the error code irrespective of whether they try to access the content via HTTP or HTTPS.

- This standard is a prime example of an Internet protocol enabling common policy objectives (in this case, transparency) to be implemented across the world. However, as with all IETF standards, the implementation of the 451 status code is voluntary. So, how widely it is used will likely depend on a number of factors, including a legal/political regime that does not penalize transparency, the willingness to be transparent and the capability to implement.

- It is possible that status code 451 code could be used for other purposes (e.g. to mislead users as to the reason for the content being blocked), especially as "legal reasons" is not defined.

- It is also possible that content providers and intermediaries who are required to block content for legal reasons to be asked or compelled to use another status code (e.g. 404). In these circumstances, content providers and intermediaries should include information in their transparency reports to indicate whether this is happening, by, for example, stating: "We have/have not been required to replace 451 by other status codes."

- There may be a temptation in some cases of the implementation of status code 451 to include the ability to identify and/or track the users that visit a web resource that has been blocked. This raises significant privacy issues.

- The usage of HTTP status code 451 might lead to an increase in blocking because it makes analyzing compliance easier.

## 10. What are features of a blocking reporting infrastructure that would be useful?

- The reporting format needs to cover information enough to satisfy transparency and offer insight about possible misuse of 451 error as a vehicle for censorship.

- Transparency requirement will be better served through standardization of fields and descriptions. Currently many

implementations for HTTP status code 451 do not provide the reason for blocking. This could be attributed to the fact that the different needs are not sufficiently documented in RFC7725. This could be fixed by adding fields in the header. Useful categorization fields to accurately describe content blocked by legal reasons are:

- Identification of the legal source on which the blocking request is based.

- Identification of the complainant/requestor if is an institution (not if individual because of privacy concerns). It could be useful to identify in this field if the request comes from a private or public entity, and in if there is a judicial order involved, or a law enforcement or other type of governmental request.

- Description of blocked content (example: 'Non-consensual sexually explicit imagery'). It could be helpful to have suggested fields that standardize type of content in order to make easier the analysis and the evaluation about eventual challenge of the use of error 451 for the specific content removal.

- Determination of the geographical scope of the blocking. Increasingly blocks are being implemented at the level of the city or province. Therefore country codes may not be sufficient to describe the geographical scope.

- Date of block order and time-period for which the block has to be enforced.

- Date of start serving HTTP status code 451.

- Link to the final decision (if available). Again this should only be the case when the complainant is not an individual.

- Contact information for relevant authority for the purposes of verification of procedural stage and appeal or redress opportunities.

## 11. What features of blocking events are supported by the existing 451 status code, and what features do we need to add?

- Guidance on the representation of HTTP status code for subresources in browsers

- Guidance on the implementation of HTTP status code 451 could lead to an increase in adoption. RFC7725 provides high level advice but still leaves space for interpretation. An implementation

guide in conjunction with an adoption campaign might lead to increased adoption.

- [RFC7725] does not clarify whether HTTP Status Code 451 is only meant for respones to GET/HEAD requests or also for POST/HEAD requests.

- Guidance on a HTTP link header to indicate that a resources that is linked on the page, but not loaded, is no longer available for legal reasons.

## 12. Appendix: Legal Realities

In the light of the use cases outlined above underneath we are providing an overview of legal frameworks in a number of countries that could be used to make a blocking request. This is to show that a reference to a the description of blocked content, the legal source on which the blocking order or request is based and the authority that is makes the order or request is crucial in understanding the context and nature of the blockage.

## 13. Russia

Blocking by the government:

### 13.1. Federal Law of 27 July 2006

Law No. 149-FZ on Information, Information Technologies and Protection of Information and its amendments:

- "Blacklist" law 139-FZ (2012) - allowing to block websites if they appear to have dangerous information for children such as information about suicide and drugs. The blocking was often done by keyword so as a result one of the biggest wiki sites in Russia (Lukmore) was accused of drugs propaganda, an online encyclopedia (Absurdopedia) was accused of suicide propaganda and an online game was blocked because on it's forum somebody used a word "drug".

- "Anti-pirate" law 187-FZ (2013) - easier way for the government to block access to websites if they are suspected in any wrongdoing. The amendment also allows blocking by IP address. Leads to the blockage of portals such as OpenSharing.org

- The law 398-FZ on immediate blockage of websites at the request of Prosecutor General (2013).

- "Bloggers' amendment" 97-FZ (2014) - bloggers with more than 3000 need to register as mass media ("information distributors") and have the same responsibilities (including on what their readers post in comments).

- Data localization law 242-FZ (2015) all companies collecting personal data of the Russian citizens must store that information on the servers within Russia

- The laws against extremism that have been updated throughout the past 5 years expanding the term "extremism" and making the punishment tougher (jail terms for posting and reposting) as well as blocking. These laws have been used widely after the conflict in Ukraine. Some people got jail sentences and resources were being blocked for spreading information sympathizing with the Ukrainian side. Such laws are particularly vague and "extremism" is very laxly defined. For example, "...extremist materials, as well as information propagating racial, national or religious hatred or enmity or hatred towards any social group."

### 13.2. "Yarovaya laws"

This law was approved by the Parliament and, if passed, will oblige messaging apps to store messaging history and decrypt messages at prosecutors' request.

## 14. Chile

### 14.1. Blocking by courts

The Law No. 20.435 (Copyright Act reform from 2010) contains a notice and take down procedure, for copyright infringements under which a court order is required -instead of a private notice like happens in the DMCA- to have content taken down. A Supreme Court decision from 2016 held that it was possible to request a news oulet to remove content in its website to enforce the constitutional right of privacy, when the data is no longer relevant and it availability on the network cause harm to the data subject. The case was controversial because the information was about a public servant condemned in a pedophilia case. This decision has been used to enforce a kind of 'right to be forgotten' for lower courts since the Supreme Court decision, but there is a lack of general legislation that clarify this cause of removals. On the other hand, the Law No. 20.453 tackles intermediary non-interference from the perspective of users by adding to the general rules within the General Telecommunications Act (Law No 18.168) new rules for internet service providers. Among those rules the internet service providers "shall not block or interfere in any way with the rights of the user to use

any content, application or service on the internet; but they may take traffic management measures or block contents upon user requests (and to their cost)".

## 15. Iran

### 15.1. Blocking by government

The Committee Charged with Determining Offensive Content (CCDOC) is the official authority on censorship and blocking of web content in Iran. The Supreme Council of Cyberspace (SCC), established in 2012, develops policies related to cyberspace governance. However, blocking and filtering directives originate from various levels of the government, including through direct orders by the judiciary independent of the SCC and CCDOC. Other organizations involved in the censorship process include the Iranian Cyber Police (FATA) and the Telecommunication Company of Iran. By national law, the Telecommunication Company of Iran (TCI) is the exclusive provider of Internet bandwidth in the country. All ISPs have to purchase bandwidth from TCI and are legally bound to use censoring software. Such a system enables a centralized filtering program for all Internet traffic in the country.

### 15.2. Blocking by courts

In Iran, freedom of expression is regulated by the Penal Code and the Press Law of 1986. The Press Law was amended in 2000 to mandate that publishing online without a license was grounds for blocking, effectively censoring services such as Google, Facebook and Twitter. Iran also has Internet-specific laws, such as the 2001 resolution called "Regulations and Conditions Related to Computerized Information Networks" that ordered that ISPs remove 'offensive' websites and mandated the use of filtering technology. The main law in terms of applicability to Internet censorship is the Computer Crimes Law (CCL) of 2009. CCL prescribes articles that provide for content-based restrictions on the Internet usage of Iranian citizens. Articles 21 through 23, in particular, hold ISPs liable for filtering content and reporting illegal material (as described in the articles) to a 'web crimes committee' made up of government officials. ISPs are also required to store usage data and logs about visited web pages for a window of at least six months. It is worth noting that none of the terms used in the CCL are defined strictly, potentially over-broadening its scope. There have been many cases of Iranian bloggers being prosecuted for violation of censorship laws. National Internet Project: The Iranian government has been working towards the creation of a National Internet Network which would domestically host all accessible Internet content, isolating Iranian citizens from the World Wide Web. Implementation of the national network would make it

easier for the government to block services and web pages through measures such as intelligent filtering. Already the use of social networking platforms such as Facebook, Instagram and Viber is heavily monitored and controlled.

## 16. India

### 16.1. Blocking by the government

Under Section 69A of Information Technology Act 2000, the executive branch of the government has "the power to issue directions for blocking for public access of any information through any computer Resource". According to the law, any person can send a block request to a Nodal Officer. These Nodal Officers should be designated in all government entities to deal with block requests. The request is then approved by the state or central Chief Secretary. This step is not required if the Nodal Officer has initiated the blocking procedure without any complainant. The request is then forward to the head of CERT-IN. If it is not a public emergency, the persons or intermediaries should be given 48 hours to respond. But this is not required if the emergency provision has been invoked, but the block list still has to be reviewed by "Committee for Examination of Request" within 48 hours after the block been issued. The block lists are usually issued directly to ISPs and are marked confidential and are implemented unevenly with some ISPs providing sparse details if users try to access the blocked resources and other ISPs returning a 404 Error Code.

### 16.2. Blocking by courts

Increasingly Indian courts are issuing ex-parte John Doe orders for website blocking. These orders can be issued by courts for any illegal content. There are around 30 different laws that place reasonable restrictions on the right to free speech in India. For example: The Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act, 1989, The Prenatal Diagnostic Techniques (Regulation and Prevention of Misuse) Act, 1994 and The Juvenile Justice Act, 2000. Some of these laws have multiple provisions that regulate speech for ex. the Information Technology Act has 6 sections and the Indian Penal Code has 10 sections. Once a court order has been obtained, the order can be sent to Secretary of the Department of Electronics and Information Technology who will then forward it to ISPs. Or alternatively complainants could also send court orders directly to ISPs without following the procedure described above.

### 16.3. Takedowns by web sites

Under Section 79 of the Information Technology Act 2000, both the government and private parties can send take-down notices to web sites. Intermediaries can ignore private party take-downs without losing immunity but take-down notices from the government have to be complied with. Under Section 52(1)(c) of the Indian Copyright Act, take-down notices can be sent to websites who are engaged in infringement but they need to be followed by court orders otherwise the content can be reinstated.

## 17. United States of America

### 17.1. Section 512 of the DMCA

The United States Digital Millenium Copyright Act (DMCA) has a provision that has greatly shaped the landscape of online content [Quilter]. Section 512 of the DMCA has a "notice and takedown" procedure that copyright holders can use to assert that a piece of copyrighted material has been posted against their wishes and that it should be taken down. Under this provision, after a website operator receives a 512 notice, it must: 1) remove the material "expeditiously"; 2) notify the poster that someone has alleged copyright infringement in that material and that the material has been removed; and 3) send any "counternotices" from the poster - objections from the poster to claims of copyright - to the original complaintant. The complaintant must notify the website operator that it has filed a lawsuite within 10-14 days or the website can reinstate the removed material.

### 17.2. Other US-based forms of takedown

There are a number of other legal methods that are used with much less frequency in the United States:

- Defamation: Under US law, balancing the freedom of speech in the US constitution is also a right to be free from untrue attacks on one's reputation. Threats and lawsuits are regularly filed claiming statements are untrue and reputationally damaging.

- Rights of publicity: The United States has a number of States that recognize a "right of publicity", typically a right enjoyed by celebrities and public figures to limit the ability of others to use their likeness, name, or recognizable features for commercial purposes.

- Non-consensual sexually-explicit imagery: A number of content providers and online content hosts (intermediaries) have begun to

honor request to take down material that may include sexually-explicit imagery that was either captured without consent or shared online without consent (cite).

- Mugshot images: Images taken in the process of a law enforcement arrest or detention have increasingly been subject to state-based regulation in the United States, recognizing that people may suffer undue reputational harm from the display and searchability of this kind of content [ElManzalawy].

- Trademark-based takedowns: A US law, The Anti-cybersquatting Consumer Protection Act (ACPA), protects the owners of trademarks from abuse by entities "cybersquatting" on domain names that contain their trademarks (cybersquatting is proactively registering a domain name to demand substantial fees from the trademark holder). Trademark holders can use the remedies in this law to request cancellation or transfer of the domain name as well as damages.

- E-Commerce Patents: Because software can be patented in the United States, there are regular claims made by patent holders against online content and services that they claim infringe their patent.

## 18. Informative References

[Censys] Durumeric, Z., Adrian, D., Mirian, A., Bailey, M., and J. Halderman, "80.http.get.status_code: 451 - Censys", 2017, <https://www.censys.io/ipv4?q=80.http.get.status_code%3A+451>.

[ElManzalawy] El Manzalawy, M., "Should the Mugshot Industry be Regulated? States Push Legislation to Protect Individuals from Disproportionate Reputational Harm", 2017, <https://www.lumendatabase.org/blog_entries/789>.

[Facebook] Facebook, inc., "How do I add or edit country or age restrictions for my Page?", n.d., <https://developer.github.com/changes/2016-03-17-the-451-status-code-is-now-supported/>.

[Github] Torikian, G., "The 451 status code is now supported", 2016, <https://developer.github.com/changes/2016-03-17-the-451-status-code-is-now-supported/>.

[Quilter] Urban, J., "Efficient Process or Chilling Effects? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act", 2005, <https://www.law.berkeley.edu/files/Chilling_Effects_Report.pdf>.

[Reddit] Turkey Blocks, "LGBTI sections disappear as Reddit complies with 100% of Turkey censorship orders", 2017, <https://turkeyblocks.org/2017/04/04/lgbti-sections-disappear-as-reddit-complies-with-turkey-censorship-orders/>.

[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>.

[Twitter] Twitter, inc., "Country withheld content", n.d., <https://support.twitter.com/articles/20169222#>.

[Youtube] Wikipedia, "Censorship of YouTube", 2017, <https://en.wikipedia.org/wiki/Censorship_of_YouTube>.

## Authors' Addresses

Sunil Abraham
CIS India

EMail: sunil@cis-india.org

Maria Paz Canales
Derechos Digitales

EMail: mariapaz@derechosdigitales.org

Joseph Lorenzo Hall
CDT

EMail: joe@cdt.org

Olga Khrustaleva
American University

EMail: ok4193a@student.american.edu

Niels ten Oever
ARTICLE 19

EMail: niels@article19.org

Christine Runnegar
ISOC

EMail: runnegar@isoc.org

Shivan Kaul Sahib
Cisco Systems

EMail: shivankaulsahib@gmail.com