Marc Perkel
Founder – Church of Reality
7498 Chestnut St.
Gilroy CA. 95020
415-987-6272 – marc@perkel.com

PLAINTIFF, IN PRO PER

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SANTA CLARA

MARC PERKEL, Plaintiff, vs. GOOGLE INC., Defendant	Case No.: COMPLAINT FOR TEMPORARY RESTRAINING ORDER, PRELIMINARY, AND PERMANENT INJUNCTIONS, AND FOR COURT COSTS

Plaintiff alleges:

1. Plaintiff, Marc Perkel is, and at all times mentioned in this complaint was, a natural person residing in Santa Clara County.

2. At all times alleged herein, Plaintiff is the Founder of the Church of Reality, a religion. Plaintiff is the registered owner of the domain churchofreality.org, Plaintiff is the system administrator / web master for his churchofreality.org web site as well has several hundred other web sites on the same server. Plaintiff also has many free speech web sites of his own and Plaintiff provides web services to many other people for free, and for profit, for free speech purposes. Plaintiff

bears all costs associated with keeping his web sites and the web sites of his friends and customers online.

3. Defendant Google Inc. is, and at all times mentioned in this complaint is, a corporation located in Mountain View California, Santa Clara county. Defendant is the publisher of the world's most popular web browsing software named “Chrome Browser”, which is used by over a billion people across the world to view web pages. Defendant is also the owner of the “Google search engine” which allows billions of people to locate and access the content that they are interested in. Defendant controls the algorithms of said search to determine which web sites are returned for a given user search and which web sites are accessible (web page ranking) through their search engine. Through their web browser software and search engine Defendant can make sites not appear in search results at all, or have a lower ranking than its relevance would indicate. Defendant also has the power to display warnings on web pages that the Defendant considers dangerous. Defendant has the ability to effectively banish the Plaintiff's web site(s) from the internet for billions of people who use Defendant's search engine and web browser.

4. Defendants is sued in this complaint under fictitious names Their true names and capacities are unknown to plaintiff. When their true names and capacities are ascertained, plaintiff will amend this complaint by inserting their true names and capacities herein. (Plaintiff is informed and believes and thereon alleges, that the fictitiously named defendant is responsible for the occurrences alleged in this complaint.)

CAUSE OF ACTION

(For Temporary Restraining Order, Preliminary and Permanent Injunction Against Google Inc)

5. On August 17th 2017, Defendant wrongfully and unlawfully sent Plaintiff 3 similar email messages (Attachment A) stating the 3 of his web sites, (although this really applies to all of the plaintiff's web sites) will be censored by the Defendant. One of those web sites was the Church of Reality. Plaintiff asserts the following facts constituting Plaintiff's affidavit:

a) In said emails Defendant threatens to distribute a new version (version 62) of its Chrome Browser starting in October of 2017, and;

b) Chrome version 62 will show a “NOT SECURE” warning in their Chrome Browser misrepresenting that Plaintiff's web site is dangerous to the viewer, and

c) Defendant stated in said email that, “The new warning is part of a long term plan to mark all pages served over HTTP as 'not secure'”, and;

d) the wording “NOT SECURE” is a knowingly false and libelous representation to the world by the Defendant defaming the Plaintiff's web site is not safe or dangerous and should be avoided, and;

e) Defendant has made public statements that web pages that use HTTP protocol instead of HTTPS protocol will get a lower search ranking and will therefore not appear in Google search results when users are looking for information which would otherwise be displayed if the Plaintiff used HTTPS protocol, and;

f) the Defendant is a monopolistic entity that is so big, and whose browser and search engine are so ubiquitous, that it can effectively block access by billions of people across the world to Plaintiff's web sites, through its Chrome browser and its search engine settings, and;

g) Plaintiff refutes Defendant's assertion stating that HTTP protocol is neither insecure or dangerous, and Plaintiff asserts that the Plaintiff's web sites will become more secure merely by changing protocols from HTTP to HTTPS, and;

h) the Defendant is demanding the the Plaintiff be forced under threat of having his church web site labeled dangerous to convert said web site to HTTPS protocol, and;

i) conversion to HTTPS protocol involves a great amount of time and expense in buying and maintaining digital certificates, and;

j) HTTPS exposes Plaintiff's web site visitors to privacy abuses in that browser certificate revocation requests are sent to certificate authority not encrypted and can be used by third parties or malicious actors to monitor and track visitors to Plaintiff's web sites, and;

k) that the Defendant's labeling of Plaintiff's web sites as “NOT SECURE” is the equivalent of digital libel, and;

l) Defendant is offering a purportedly free remedy of obtaining free certificates, but the free certificate source (Let's Encrypt), however LE only offers 90 day certificates and there's no guarantee that they will continue to offering certificates for free in the future forcing Plaintiff to spend additional tens of thousands of dollars purchasing certificates from certificate vendors, and;

m) once a web site is converted to HTTPS the web site can never be converted back to HTTP and will therefore forever need certificates, and;

n) no other web browser by any other vendor labels HTTP protocol as NOT SECURE, and;

o) no other search engine penalizes web site ranking based on the use of HTTPS vs. HTTP protocol, and;

p) the Defendant is not a regulatory agency and is usurping the powers of a regulatory agency, and;

q) the above actions threatened by the Defendant will deprive the Plaintiff of his constitutional right to free speech, religious liberty, and/or cause him to have to expend a great

amount of his time and at great expense to implements HTTPS protocol for which there is no Reality based reason to do so.

6. HTTP protocol has been the standard for browsing the Internet since the beginning of the World Wide Web (WWW). As more businesses adopted using the WWW to transmit sensitive private information a new web protocol was developed called HTTPS which added two security functions, encryption and identity authentication. Encryption prevents a third party from intercepting communication in transit, and authentication ensures that the web site you think you are connected to is authentic. Although encryption could have been implemented independently, for some reason HTTPS links these two functions together. HTTP protocol is easy to implement and doesn't require certificates.. A web site can be created in minutes and left in tact online for decades with no maintenance. HTTPS however is very different.

Generally certificates need to be purchased from a certificate authority who verifies the identity of the domain owner and issues them a digital certificate that web browsers, like Google's Chrome browser, can recognize as authentic. This prevents web sites from impersonating banks to steal your money, for example. Certificates can be costly depending on the certificate vendor and the certificate is issued only for a limited amount of time set by a digital expiration date. If a certificate expires, the web site is no longer accessible to be viewed by the world.

The Plaintiff however has hundreds of web sites containing static information and do not have user accounts containing publicly available any information that does not need to be protected. Most of these sites are read only and the information there is accessible to anyone. Thus encrypting the web site adds no benefit and at great expense.

Defendant has however offered a remedy, in a link within their emails to an organization called “Let's Encrypt” (LE) with a link in the email they sent to this web site. This site is a donation

supported non-profit organization that issues certificates for free. However, those certificates are only good for 90 days and have to be renewed and replaced before the 90 day expiration is up. LE makes no warranty that their service will be free forever and there is no other source of free certificates available. If LE changes their policy, fails to get donations, has their private encryption keys stolen, or fails a security audit then within 90 days all their certificate will quit working leaving Plaintiff to spend some $10,000/year for commercial certificates that Plaintiff neither wants or needs.

Defendant expects Plaintiff to trust LE but LE isn't a real entity in that it doesn't have any technical support contacts on it's web site, nor does it have any employee list, nor does it have a telephone or fax number, nor do they publish a street address, and all the published email addresses are inaccessible. Even if however Plaintiff believed he could get an infinite supply of free certificates forever (681 needed every 90 days), the work involved in maintaining and replacing certificates is an undue burden unjustly and illegally imposed by the Defendant on the Plaintiff.

Both HTTP and HTTPS have their advantages and disadvantages and in some cases HTTPS is the right choice and in some cases HTTP is the right choice. The issue before this court is, “Who gets to make that choice?” Does the Defendant have a right, through monopolistic coercion, to act as a regulatory agency, to force their choice on the Plaintiff's web sites?

And ultimately, who is Google to impose their will through their monopolistic powers to tell the founder of the Church of Reality what protocol he is required to use? Defendant has the burden of proving that the Plaintiff's web sites would be significantly more secure to the extent that it justifies their threat of representing to the world that the Plaintiff's web sites dangerous merely because of the use of HTTP, rather than HTTPS protocol.

7. Defendant's threatened wrongful conduct, unless and until enjoined and restrained by order of this court, will allow the Defendant to electronically libel the Plaintiff's religious web sites and free

speech web sites, and will cause the Plaintiff great and irreparable injury in that Plaintiff's free speech rights and religious freedom rights will be infringed or that the time and expense required to comply with Defendant's unlawful demands would be prohibitively expensive.

WHEREFORE, Plaintiff prays judgment against Defendant as follows:

1. For an order requiring Defendant to show cause, if any they have, why they should not be enjoined as set forth in this complaint, during the pendency of this action;

2. For a temporary restraining order prohibiting Defendant from distributing Chrome version 62 with the “NOT SECURE” warning.

3. For a preliminary injunction, and a permanent injunction, all enjoining Defendant, and their agents, servants, and employees, and all persons acting under, in concert with, or for them from:

a. distributing Chrome version 62 with threatened “NOT SECURE” warning;

b. continuing their long term plan to mark all pages served over HTTP as “NOT SECURE”, including prohibiting the use of emails threatening such action;

c. reducing the search ranking of web sites based on the use HTTP protocol;

3. Plaintiff is not a lawyer, and therefore this complaint should be interpreted by the court expansively. The Church of Reality is a religious organization and the Strict Scrutiny rules under the Religious Freedom Restoration Act (42 USC 2000bb) apply to this action, and ;

4. For costs of suit incurred in this action; and

5. For such other and further relief as the court deems proper.

DATED: October 9, 2017

_____
Marc Perkel
In Pro Per

ATTACHMENT A
Letter from Google

Google Search Console

Chrome will show security warnings on http://www.churchofreality.org

To owner of http://www.churchofreality.org,

Starting October 2017, Chrome (version 62) will show a “NOT SECURE” warning when users enter text in a form on an HTTP page, and for all HTTP pages in Incognito mode.

The following URLs on your site include text input fields (such as < input type="text" > or < input type="email" >) that will trigger the new Chrome warning. Review these examples to see where these warnings will appear, so that you can take action to help protect users’ data. This list is not exhaustive.

http://www.churchofreality.org/wisdom/welcome_home/

http://www.churchofreality.org/wisdom/flying_spaghetti_monster/

The new warning is part of a long term plan to mark all pages served over HTTP as “not secure”.

Here’s how to fix this problem:

Migrate to HTTPS

To prevent the “Not Secure” notification from appearing when Chrome users visit your site, only collect user input data on pages served using HTTPS.

Read about HTTPS

Need more help?

- Learn more about this change in the blog post Next Steps Towards More Connection Security.
- Learn how to Secure your site with HTTPS.
  Ask questions in our forum for more help - mention message type [WNC-10038795].
- Google Inc. 1600 Amphitheatre Parkway Mountain View, CA 94043 | Unsubscribe from this type of message
  Add partners who should receive messages for this Search Console account.