

**Federal Trade Commission**  
**Hearings on Competition and Consumer Protection in the 21st Century**  
**(September 26, 2018)**

**Supplemental Public Comments submitted by the CA Security Council (CASC)**

The CA Security Council (CASC), [www.casecurity.org](http://www.casecurity.org), submitted Public Comments to the FTC's "Hearings on Competition and Consumer Protection in the 21st Century" on August 31, 2018.

There have been important new developments since that time, and so CASC is hereby submitting Supplemental Public Comments to the FTC.

**1. Google is moving faster than expected to remove website identity information from consumers in Chrome:** In our previous submission, we stated the following about Google's plan to remove all identity information about websites from consumers in the Google Chrome user interface (UI) address bar:

**"Google has announced** that Chrome 72 in January 2019 will remove all positive UI security indicators, probably including the EV UI (company name, country, and corporate serial number) shown in the screen shots below for [bankofamerica.com](http://bankofamerica.com). If this happens, this will mean consumers will no longer be able to tell the difference between their bank's *real* website with an EV certificate (containing confirmed identity and location information), and a *fake* phishing site with an anonymous DV certificate (containing no confirmed identity or location information) pretending to be their bank. They will be tricked."<sup>1</sup>

In fact, Google did not wait for Chrome 72 next year to start making website identity information harder for consumers to see, but has already started this month by altering its Extended Validation (EV) UI to make it less visible to consumers in Chrome version 69. Here are the facts.

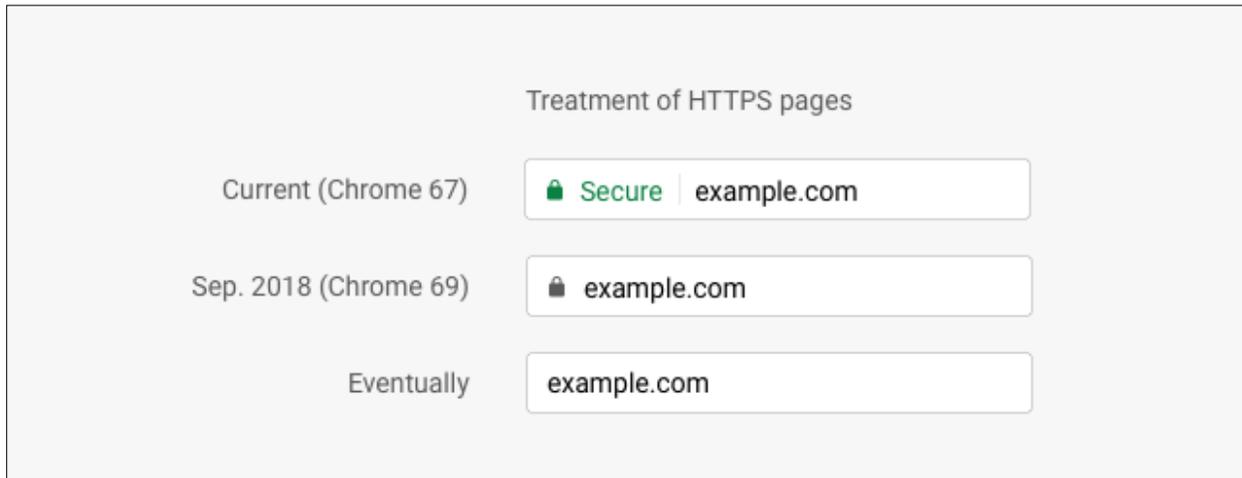
Google is systematically following a path to remove all strongly verified identity information in its web browser UI. Google's plan, announced in May 2018, is to gradually reduce the information it presents to consumers in the Chrome UI over the balance of the 2018:

"Users should expect that the web is safe by default, and they'll be warned when there's an issue. Since we'll soon start marking all HTTP pages as "not secure", we'll step towards removing Chrome's positive security indicators so that the default unmarked state is secure. Chrome will roll this out over time, starting by removing the "Secure" wording and HTTPS scheme in September 2018 (Chrome 69).

---

<sup>1</sup> See page 4 of prior CASC submission "(a) Summary of CA Security Council Public Comments to FTC 30 Aug 2018"

[Google then presented this screen shot of how the Chrome UI will gradually remove information from users:]<sup>2</sup>



Google's target end-state is to show a consumer only the domain name or URL of the website, and nothing more. Unfortunately, this is exactly the type of browser UI that phishers love (one with minimal information that can be easily imitated to fool consumers) – look again at the *real* PayPal website below on the *left* (which is strongly identified by an EV certificate with confirmed organization information displayed to the consumer in a distinctive EV UI) and a fake *phishing* site on the *right*, [www.paypal.com.summary-spport.com](http://www.paypal.com.summary-spport.com), which is imitating PayPal in a UI where only the phishing site's URL is displayed to consumers in the address bar (the full URL is truncated) – a consumer can't really tell the difference between the two websites based on the URL alone, and so is likely to be tricked by the phisher into revealing consumer username and password information once the distinctive EV UI is removed by Google later this year:

**PayPal Example – real PayPal site (EV certificate) vs. phishing site (DV certificate)**  
**August 2018**

**Real PayPal Site**



**URL:** [www.paypal.com](http://www.paypal.com)

**EV Site:** Shows the organization name and country. This information and UI will *disappear* in Chrome 72 in January 2019

**Phishing PayPal Site**



**URL:** [www.paypal.com.summary-spport.com](http://www.paypal.com.summary-spport.com)

**DV Site:** Only shows the URL, which can fool users

<sup>2</sup> <https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html>

The two sites, real and fake, will look substantially the same after Google removes the EV UI in Chrome 72. Google has even admitted this will be a problem for consumers – see Section 2 below.

Why does this matter? Remember, Extended Validation or EV certificates are the highest level of identity confirmation that a website can have, and are used extensively by banks, hospitals, and even government agencies like the US Senate, [www.senate.gov](http://www.senate.gov). Since 2008 these EV certificates have received their own distinctive **green** EV UI in most browsers (including Chrome) showing consumers both the confirmed **company name** and its **country of operation**. The EV UI used to be mostly **green**, which helped consumers know that the website’s identity had been strongly confirmed by a trusted third party – but with the release of Chrome 69 in September, Google has now dumbed-down the website identity information it shows to consumers to a dull gray obscured with a gray background. EV websites are now hard to tell apart from anonymous DV websites, which is apparently a step on Google’s path to removing all positive indicators in the Chrome UI by Chrome 72. The problem we predicted in our earlier public comments has already arrived – Google has already made it hard for consumers to see identity information today, five months ahead of schedule.

Here are two examples of this change – the EV UI in Chrome for the US Senate’s own website, [www.senate.gov](http://www.senate.gov), as it appeared earlier this summer in Chrome 68 (**green**) and the new EV UI for the same US Senate website in Chrome 69 (**dull gray with a gray background**):

#### Chrome 68 (July 2018)



#### Chrome 69 (September 2018)



Again, consumers will find it increasingly hard to notice that there is confirmed identity information in the EV certificate securing a website – here is the confirmed identity information that consumers can see if they simply click on the padlock that assures them they really are at the website of the US Senate:

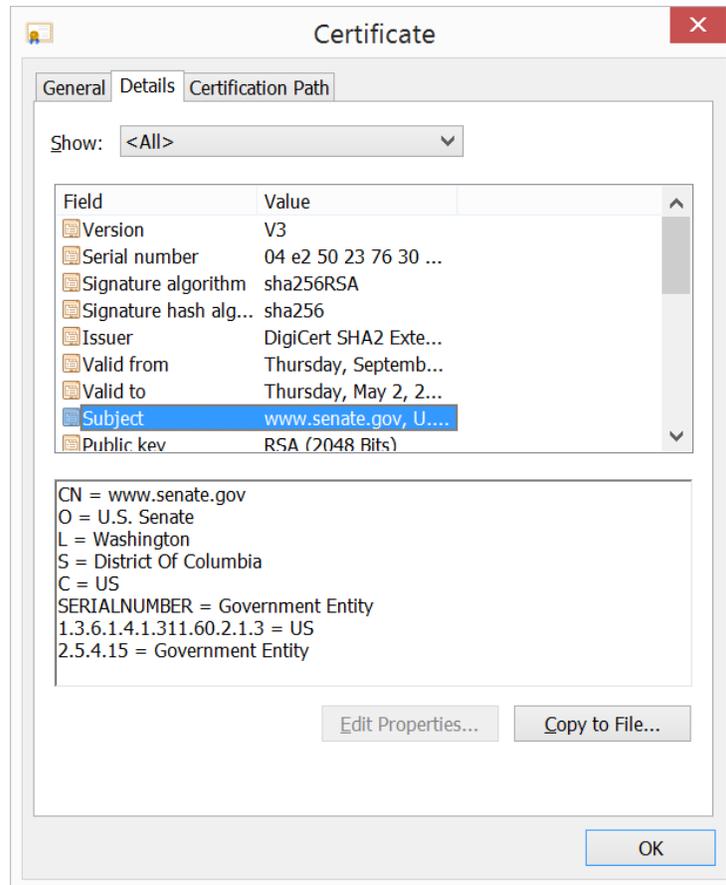
- CN =** This is the domain or URL for the website, such as [www.senate.gov](http://www.senate.gov)
- O =** This is the confirmed Organization name, like “**U.S. Senate**”
- L =** This is the Locality or city where the Organization is located, like “**Washington**”
- S =** This is the State or district where the Organization is located, like “**District of Columbia**”
- C =** This is the Country where the Organization is located, like “**US**”

**SerialNumber** = This is the Incorporation Number for corporations, otherwise shows as “**Government Entity**” for entities like the US Senate

**State/Country of incorporation (1.3.6.1.4.1.311.60.2.1.3)** = This is normally the State of Incorporation for corporations, otherwise just “**US**” for Federal government entities

**Type of entity (2.5.4.15)** = This is Organization type, like “Private Organization” for corporations and “**Government Entity**” for government bodies like the US Senate

Here is a screen shot of the actual data that is cryptographically locked into the EV certificate for the US Senate’s actual website, [www.senate.gov](http://www.senate.gov):



Why wouldn't Google want consumers to *know* that this information is present in the SSL server certificate securing the website of the US Senate? Hiding identity information from consumers is exactly the *wrong* thing to do at a time when encrypted phishing attacks using look-alike domains (URLs) and fake websites are rising exponentially – instead, this is the time to give consumers *more* information and control over the websites they visit, not less.

You can see larger images of the US Senate’s actual home page, [www.senate.gov](http://www.senate.gov), in Chrome 68 (with the distinctive **green EV UI**) and in the new Chrome 69 (with a **dull gray UI and a gray background**) on [Appendix A](#). Consumer confusion will only get worse as Google moves toward its ultimate goal of removing *all* identity information from the Chrome UI in Chrome 72 except for the URL, which is set to occur this January, 2019. Google should *pause* and reconsider this unfortunate plan.

## **2. Google appears totally confused about whether removing information from consumers in the Chrome UI is a good thing or a bad thing, and appears to be struggling for a solution**

Recently there has been an unsettling display of confusion by Google in whether *removing* information from consumers in the Chrome UI is a good thing or a bad thing, and Google appears to be struggling for a solution – but sadly, it is marching forward with the complete removal of all positive UI information in Chrome 72 while it tries to decide what the *right* solution actually is. This split personality approach will likely cause harm to consumers in the meantime, and increase the likelihood that phishers will succeed in stealing valuable, confidential consumer data because of changes to the Chrome UI. **Google should *pause* while it makes up its mind, and restore the *green EV UI* in the interim.**

As we previously reported, Google indicated more than two years ago that it planned to remove the EV UI from Chrome. Google is the dominant browser in the US, with a market share of nearly 68%,<sup>3</sup> and it stated its plans earlier this year very clearly, including its intention to remove all positive UI security indicators by January 2019 with the release of Chrome 72.<sup>4</sup> See again this statement from May 2018:

“Users should expect that the web is safe by default, and they’ll be warned when there’s an issue. Since we’ll soon start marking all HTTP pages as “not secure”, **we’ll step towards removing Chrome’s positive security indicators** so that the default unmarked state is secure. Chrome will roll this out over time, starting by removing the “Secure” wording and HTTPS scheme in September 2018 (Chrome 69). \*\*\* ”

Google made good on its promise to begin removing positive security indicators by graying-out the EV UI in Chrome 69 released earlier this month, and it appears to be on the path to removing the EV UI entirely in Chrome 72 next January.

But then, to everyone’s surprise, **Google admitted this month that a Chrome UI that only shows consumers the URL (domain) of the website they are viewing is *not* sufficient for consumer safety, and consumers need “something more” to know the identity of the website! This is a *complete reversal* of Google’s prior position:**

### **Google Wants to Kill the URL<sup>5</sup>**

Google's Chrome browser turns 10 today, and in its short life it has introduced a lot of radical changes to the web. From popularizing auto-updates to aggressively promoting HTTPS web encryption, the Chrome security team likes to grapple with big, conceptual problems. That reach and influence can be divisive, though, and as Chrome looks ahead to its next 10 years, the team is mulling its most controversial initiative yet: fundamentally rethinking URLs across the web.

---

<sup>3</sup> [https://en.wikipedia.org/wiki/Usage\\_share\\_of\\_web\\_browsers#StatCounter\\_\(July\\_2008\\_to\\_July\\_2018\)](https://en.wikipedia.org/wiki/Usage_share_of_web_browsers#StatCounter_(July_2008_to_July_2018))

<sup>4</sup> <https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html>  
<https://blog.cloudflare.com/https-or-bust-chromes-plan-to-label-sites-as-not-secure/>

<sup>5</sup> <https://www.wired.com/story/google-wants-to-kill-the-url/>

Uniform Resource Locators are the familiar web addresses you use every day [like [www.example.com](http://www.example.com)]. \*\*\* But over time, URLs have gotten more and more difficult to read and understand. As web functionality has expanded, URLs have increasingly become unintelligible strings of gibberish combining components from third-parties or being masked by link shorteners and redirect schemes [which are used by phishers to deceive consumers]. And on mobile devices there isn't room to display much of a URL at all.

The resulting opacity has been a boon for cyber criminals who build malicious sites to exploit the confusion. They impersonate legitimate institutions, launch phishing schemes, hawk malicious downloads, and run phony web services—all because it's difficult for web users to keep track of who they're dealing with. Now the Chrome team says it's time for a massive change.

**"People have a really hard time understanding URLs," says Adrienne Porter Felt, Chrome's engineering manager. "They're hard to read, it's hard to know which part of them is supposed to be trusted, and in general I don't think URLs are working as a good way to convey site identity. So we want to move toward a place where web identity is understandable by everyone—they know who they're talking to when they're using a website and they can reason about whether they can trust them. But this will mean big changes in how and when Chrome displays URLs. We want to challenge how URLs should be displayed and question it as we're figuring out the right way to convey identity."**

If you're having a tough time thinking of what could possibly be used in place of URLs, you're not alone. Academics have considered options over the years, but the problem doesn't have an easy answer. **Porter Felt and her colleague Justin Schuh, Chrome's principal engineer, say that even the Chrome team itself is still divided on the best solution to propose. And the group won't offer any examples at this point of the types of schemes they are considering.**

So even Google is admitting that its plan to display nothing but website URLs to consumers won't work from a consumer security standpoint – yet that is the exact plan Google is implementing in its march forward to Chrome 72 next January. This makes no sense at all, and the FTC and other federal cybersecurity agencies should take action now.

We are also concerned that Google could move to a closed-end, proprietary “identity” solution that will only work within the Google environment and will not be portable to transmit and share identity information to consumers outside the Google ecosystem – in contrast, using and displaying data to consumers found in EV certificates is universal and works across all environments to protect consumers, including in Google Chrome and all other applications.

### **3. What should the FTC do now in response to these unfortunate UI changes by Google?**

Google's recent change to the EV UI in Chrome 69 is an alarming and dramatic demonstration of Google's misguided plan to remove security information from consumers as it progresses to Chrome 72 in January 2019 – when all positive information will be removed from the Chrome EV UI. This is not the time for Google to take away identity and security information from consumers, it's time to give consumers more information and more control over the websites they visit, not less.

**What should the FTC do in response? We repeat our conclusion from the first Public Comments we submitted last month:**

“In the coming weeks, ask Google to *pause* in its plans to remove all positive UI security indicators (including removal of identity information) until the FTC has time to gather information and consider the additional actions below (and until the FTC has a chance to respond to Congress). Positive security indicators indicating the identity and location of the website owner should *not* be allowed disappear from Google Chrome this January – in fact, fast action by the FTC is needed because *it may be difficult for Google to reverse course* once it announces definitively that it’s removing the EV UI in Chrome 72 next January.

“Google is by far the dominant browser in the US, with a market share of *nearly 68% and growing* – any action Google takes to remove website identity information next January could degrade website security for the majority of consumers.”

We strongly urge the FTC to take action now, before more consumers are harmed by phishing attacks using deceptive URLs and fake websites in Google Chrome.

## Appendix A

*Former* US Senate's home page in Chrome 68 with the distinctive **green EV UI** from last summer. The EV UI really pops out and is clearly visible to consumers on the Senate's website – this helps assure them they are really at the Senate's website, and not at a fake [www.senate.gov](http://www.senate.gov) phishing page designed to steal credentials or spread false information from foreign sources.



*Current* US Senate's home page in Chrome 69 with the **dull gray UI and a gray background**, which was released in September 2018. The EV UI is nondescript and not easily visible to consumers. This could make them more easily fooled by a fake [www.senate.gov](http://www.senate.gov) phishing page designed to steal credentials or spread false information from foreign sources. Why did Google make this unfortunate change?

