



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

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

The CA Security Council (CASC), [www.casecurity.org](http://www.casecurity.org), hereby submits the following Public Comments relating to the upcoming FTC *Hearings on Competition and Consumer Protection in the 21st Century*.

These Public Comments relate to the following FTC Initial Topics for Comment:

2. Competition and consumer protection issues in communication, information, and media technology networks; \*\*\*
3. The identification and measurement of market power and entry barriers, and the evaluation of collusive, exclusionary, or predatory conduct or conduct that violates the consumer protection statutes enforced by the FTC, in markets featuring “platform” businesses; \*\*\*
5. The Commission’s remedial authority to deter unfair and deceptive conduct in privacy and data security matters; \*\*\*
9. The consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics; \*\*\*
11. The agency’s investigation, enforcement and remedial processes. \*\*\*

**1. Who we are:** The CA Security Council (CASC) is comprised of leading global Certificate Authorities (CAs) that are committed to the exploration and promotion of best practices that advance trusted SSL/TLS digital certificate deployment and CA operations as well as the security of the internet in general. CASC works collaboratively to improve understanding of critical policies and their potential impact on the internet infrastructure.

Membership in the CASC is available to publicly trusted SSL certificate authorities that meet the CASC’s reputation, operation, and security requirements. Current CASC members include Comodo CA, Entrust Datacard, GlobalSign, GoDaddy, and Trustwave.

**2. The problem we are addressing:** Consumers today can tell which websites have strongly confirmed identity and which do not by simply looking at their web browser address bar. Google will be removing this identifying User Interface (UI) in Chrome 72 in January 2019.

Google’s Chrome browser currently has a market share of approximately 70%, and so strongly dominates the market. Once Google removes the identity UI from Chrome, *all websites will look*

*the same* – those with strongly confirmed identity (which have virtually no fraud or phishing), and those which are anonymous (where 99.8% of encrypted phishing occurs today). There will be no way to tell them apart, and consumers will be hurt.

*Website identity is important for protecting consumer security, including from foreign bad actors.* Google should not remove or hide website owner identity information from consumers, but instead should add more information for consumer protection. The FTC should take corrective action pursuant to its powers under the FTC Act, 15 USC §41 et seq. to prevent unfair or deceptive acts or practices by fraudsters who use the platforms established by browsers such as Chrome to defraud consumers.

We hope the FTC will exercise its jurisdiction to protect consumers from fraud using the internet as the means of communication. The FTC seems to be the most appropriate agency to take up such a challenge.

**3. Public Comments submitted:** The CA Security Council is hereby submitting the following Public Comments (attached) relating to the Initial Topics for Comment listed above:

(a) *“Summary of CA Security Council Public Comments to FTC 30 Aug 2018.”* This is a shorter summary of our Public Comments to the FTC, with illustrations.

(b) *“CA Security Council Public Comments to FTC 30 Aug 2018.”* These are our complete Public Comments to the FTC, with illustrations.

(c) *“Fake Russian sites reinforce why public-facing government websites need EV Certificates 27 Aug 2018.”* This is a technology article based on the recent Washington Post article “Microsoft says it has found a Russian operation targeting U.S. political institutions” dated August 21, 2018, which includes examples of foreign-owned websites that imitate the real US Senate websites as well as a conservative Republican think tank, the Hudson Institute.<sup>1</sup> These are the fake domain addresses used by Russian sites to trick consumers “with the apparent goal of hacking into the computers of people who were tricked into visiting, according to Microsoft”: [senate.group](#), [adfs-senate.services](#), [adfs-senate.email](#), [hudsonorg-my-sharepoint.com](#)

**4. Our recommended actions for the FTC:** Based upon these Public Comments, we recommend the FTC take the following actions to protect consumers against internet fraud, perhaps with the support of other federal agencies concerned about cybersecurity:

1. In the coming weeks, ask Google to pause in its plans to remove all positive UI security indicators (including removal of EV identity information) until the FTC has time to gather information and consider the additional actions below. Google is by far the dominant browser in the US, with a market share of *nearly 68% and growing* – any action Google

---

<sup>1</sup> [https://www.washingtonpost.com/business/economy/microsoft-says-it-has-found-a-russian-operation-targeting-us-political-institutions/2018/08/20/52273e14-a4d2-11e8-97ce-cc9042272f07\\_story.html?utm\\_term=.6a88fc250e48](https://www.washingtonpost.com/business/economy/microsoft-says-it-has-found-a-russian-operation-targeting-us-political-institutions/2018/08/20/52273e14-a4d2-11e8-97ce-cc9042272f07_story.html?utm_term=.6a88fc250e48)

takes to remove website identity information next January could degrade website security for the majority of consumers.

2. Here is the most important step the FTC can take (and it's relatively simple to implement):

**\*\*Require browsers to display a consumer warning on any anonymous DV web page that asks consumers for their personal information, such as passwords or credit card information.\*\***

Webpages with identity certificates (OV or EV) could ask for consumer information and not receive the warning, as those sites have been fully identified. This single requirement from the FTC could substantially reduce consumer phishing attacks, as fraudsters don't want to reveal their confirmed identity on their fake phishing sites – they will only operate with the anonymity of a DV certificate. The FTC already has strict rules on Telemarketing Sales, including requiring identification of the seller – the same principle could be applied to “website browser sales” where consumer data is requested.

The guiding philosophy for internet transactions with consumers should be that consumers have the right to identity information about the websites they visit – and the FTC can make this happen. Consumers should tell websites “You don't have the right to ask me for my personal information until you first disclose your own identity to me.”

3. More generally, recommend or require browsers to use UI security indicators to show consumers when they are at a website with EV or OV identity information that has been independently confirmed by an audited third party (such as Certification Authorities). Facebook is now requiring that people who buy “issue” ads be independently identified – the same should apply to browsers. This ties in with Recommendation #2.
4. *Recommend* that *consumers* use only browsers that display website identity information in the browser UI, and require that government agencies and their vendors use only browsers that display website identity information in the browser UI.
5. Finally, require browsers to cooperate on developing common browser UI security indicator elements (as occurred with “Stop” signs early in the 20<sup>th</sup> century) and engage in consumer education so that consumers will *understand* the UI indicators across multiple browsers, whether on desktop or mobile devices. The FTC itself could convene regular meetings of the browsers, CAs, and others to help develop and maintain these common UI elements.

Thank you for your consideration. We will be happy to provide further information, including live testimony, upon request.

For further questions on these comments please contact:

Rhod Shaw, Alpine Group  
500 N. Capitol Street, NW

Washington, DC 20003  
202-547-1831  
rshaw@alpinegroup.com