Mozilla: DNS/DoH, USA FREEDOM Act, Critiquing Design and Sandboxing

By *Roy Schestowitz*
Created *25/02/2020 - 4:49pm*
Submitted by Roy Schestowitz on Tuesday 25th of February 2020 04:49:59 PM Filed under Moz/FF [1]

- **Firefox continues push to bring DNS over HTTPS by default for US users**[2]

  Today, Firefox began the rollout of encrypted DNS over HTTPS (DoH) by default for US-based users. The rollout will continue over the next few weeks to confirm no major issues are discovered as this new protocol is enabled for Firefox?s US-based users.

  A little over two years ago, we began work to help update and secure one of the oldest parts of the internet, the Domain Name System (DNS). To put this change into context, we need to briefly describe how the system worked before DoH. DNS is a database that links a human-friendly name, such as www.mozilla.org, to a computer-friendly series of numbers, called an IP address (e.g. 192.0.2.1).

- **The Facts: Mozilla?s DNS over HTTPs (DoH)** [3]

  The current insecure DNS system leaves billions of people around the world vulnerable because the data about where they go on the internet is unencrypted. We?ve set out to change that. In 2017, Mozilla began working on the DNS-over-HTTPS (DoH) protocol to close this privacy gap within the web?s infrastructure. Today, Firefox is enabling encrypted DNS over HTTPS by default in the US giving our users more privacy protection wherever and whenever they?re online.

- **Goals for USA FREEDOM reauthorization: reforms, access, and transparency**[4]

At Mozilla, we believe that privacy is a fundamental digital right. We?ve built these values into the Firefox browser itself, and we?ve pushed Congress to pass strong legal protections for consumer privacy in the US. This week, Congress will have another opportunity to consider meaningful reforms to protect user privacy when it debates the reauthorization of the USA FREEDOM Act. We believe that Congress should amend this surveillance law to remove ineffective programs, bolster resources for civil liberties advocates, and provide more transparency for the public. More specifically, Mozilla supports the following reforms...

[...]

Second, the program may not provide sufficiently valuable insights in the current threat environment. In a recent Senate Judiciary Committee hearing, the government acknowledged that the intelligence value of the program was outweighed by the costs and technical challenges associated with its continued operation. This conclusion was supported by an independent analysis from the Privacy and Civil Liberties Oversight Board (PCLOB), which hopes to publicly release an unclassified version of its report in the near future. Additionally, the shift to other forms of communications may make it even less likely that law enforcement will obtain useful information through this specific authority in the future.

And finally, some technological shifts may have made the CDR program too complex to implement today. Citing to ?technical irregularities? in some of the data obtained from telecom providers under the program, the NSA deleted three years? worth of CDRs that it was not authorized to receive last June. While the agency has not released a specific explanation, Susan Landau and Asaf Lubin of Tufts University have posited that the problem stems from challenges associated with measures in place to facilitate interoperability between landlines and mobile phone networks.

- **Critiquing Design** [5]

  This is me about 25 years ago, dancing with a yoga ball. I was part of a theater company where I first learned Liz Lerman?s Critical Response Process. We used this extensively?it was an integral part of our company dynamic. We used it to develop company work, we used it in our education programs and we even used it to redesign our company structure. It was a formative part of my development as an artist, a teacher, and later, as a user-centered designer.

  What I love about this process is that works by embedding all the things we strive for in a critique into a deceptively simple, step-by-step process. You don?t have to try to remember everything the next time you?re knee-deep in a critique session. It?s knowledge in the world for critique sessions.

- **Firefox for Mac and Linux to get a new security sandbox system** [6]

Moz/FF