

Adrienne McAdory  
Atgron, Inc.  
9435 Lorton Market St. Ste 174  
Lorton, VA 22079

July 2, 2018

National Telecommunications and Information Administration (NTIA)  
U.S. Department of Commerce  
1401 Constitution Avenue NW  
Room 4725  
Attn: Fiona Alexander  
Washington, DC 20230

To Whom It May Concern,

Please find comments and recommendations for international internet policy priorities for 2018 and beyond.

Fundamentally, the organization responsible for the stability and security of the internet, The Internet Corporation for Assigned Names and Numbers (ICANN) has failed to address the lack of a secure internet since their inception 19 years ago. The current problem with alleged Russian interference in our election can be traced to the lack of a secure internet. As the President and CEO of a company that successfully bid for a new generic Top Level Domain (gTLD) and as a contractor with the Department of Defense for over a decade, I can positively affirm through first hand experience that ICANN only dedicates resources to the stability of the internet. For the most part, ICANN acts as an extended division of Verisign which has a vested interest in maintaining the status quo. Verisign not only controls .com and other gTLDs, but more importantly, despite the creation of ICANN in 1998, Verisign still controls the root zone and any changes to the root zone. This is important because Verisign generates a significant amount of revenue from selling products to corporations and consumers to make their use of the internet more secure.

That said, maybe NTIA decided to limit ICANN's functions to only those related to the stability of the internet and that is why there is very little work or discussion of these matters at the quarterly meetings held by ICANN around the globe. These meetings consist of "working groups" of unpaid resources who all have full-time jobs, meet at these quarterly meetings and ultimately accomplish very little beyond tweaking existing policy. In 2013, both China and Russia were lobbying the United Nations to take over the functions of ICANN. Both of these countries have stopped lobbying for any control of ICANN because they are now aware the "Emperor has no clothes" and they are in the best position to exploit the vulnerabilities of the internet as long as ICANN is charged with this mission.

Recommendation 1: NTIA should release a new contract to a separate independent organization to handle the security of the internet and remove control of the root zone from ICANN and Verisign.

I hesitate to write this section because mine is a small company and I am about to make allegations against two technical giants that many would say could not be possible but I can only write about my actual experience and the data I have to prove my allegations. In 2014, I ran ads with both Facebook

and Google AdWords and discovered the same problem with both companies. Specifically, neither of their platforms filter out clicks on websites from “bots” vice clicks from personal computers and devices. When businesses are paying Facebook and Google for “clicks” on their website, they are paying for potential customers to come to the website and hopefully convert to actual customers and buy the product. You would not expect a customer to buy on the first click but maybe on subsequent clicks. That is the expectation and what Facebook and Google literature lead you to believe. As of 2014, that was not the case. I managed my own web server through my Internet Service Provider and I was able to monitor the actual clicks on my webserver so that I could monitor the clicks being billed to me by Facebook and Google. In both cases, I found the “click” numbers to be significantly inflated with both companies. I disputed the charges from Facebook and Google with American Express. Facebook did not respond to the dispute and American Express refunded \$30,000 to me as a result.

Google Adwords purported that there were 71,268 hits on my website from May 7-May 26, 2014 when my webserver logged only 811 hits to my website from Google Adwords. Upon researching the issue, I was pointed to automated bots as the problem. Ironically, when a Google customer using Google AdWords to generate ad revenue logs a large number of hits that would require Google to pay them, Google will claim that the customer used bots to create the inflated numbers and will refuse to pay the revenues owed. You might wonder why so many companies use Google Adwords and that is because the advertising companies who manage on-line advertising for large companies also benefit from the inflated numbers because they can assure their customers the ads have been “seen” when they have not.

Please note the web server logs to support these allegations can be provided upon request.

Recommendation 2: NTIA should aggressively work towards eliminating the ability for automated bots to act as revenue generators for online ad providers and to act in denial of service attacks as well.

Sincerely,



Adrienne McAdory  
President & CEO  
Atgron, Inc.