

**Federal Trade Commission**

**Hearings on Competition and Consumer Protection in the 21st Century**

*#756: Competition and consumer protection issues in communication, information, and media technology networks*

*Project Number: P181201*

August 20, 2018

Submission by Digital Citizens Alliance

In its announcement seeking public comment, the Federal Trade Commission has stated that it has particular interest in “unique competition and consumer protection issues associated with Internet and online commerce.”

The [Digital Citizens Alliance](#) is a consumer-focused group whose mission is to raise awareness among the public and policymakers about how to make the Internet safer. Digital Citizens Alliance engages with key Internet stakeholders - individuals, Internet companies, and civic leaders - to search for solutions to Internet safety issues. Based in Washington, DC, the Digital Citizens Alliance counts among its supporters the health, pharmaceutical, creative and security industries, online safety experts, and other communities such as consumer advocates focused on Internet safety.

The Digital Citizens Alliance is honored to have the opportunity to not only raise awareness around the critical challenges consumers are facing online, but also to support this Commission’s critically needed re-examination and re-evaluation of the state of consumer protection and harm resulting from the way online platforms are doing business. While the Federal Trade Commission’s review may be happening now, the safety, security and privacy issues that are hitting consumers directly have been brewing for over a decade as Google, Facebook, Twitter, YouTube, and other platforms develop and grow. We are at a point where online platforms are looking more and more like the dark web.

We are at this boiling point as a direct result of a hands-off policy coupled with an online platform business model that thrives on negative behavior. In short, the revenue model of online platforms like Google and Facebook is based on scraping or gathering as much information on users as possible. The more info they collect, the more data they can monetize with advertisers or partners. The richer the data set, the more platforms can charge for it, and the more advertisers are willing to pay for it. All this means one thing, platforms make more money the more consumers engage with content on their platforms. As such, anything that impacts the ability to collect data off of consumers directly hurts this precious revenue stream.

Identifying and then blocking or removing content means less consumer eye-balls on content, which means less data to collect, which means less valuable information to sell to advertisers, which means less revenue, and which means loss of value to shareholders and investors.

This can mean only one thing – keep bad content on a platform no matter how much it hurts consumers, since consumers are not actually the paying customer.

In short, this business model compels two things to happen repeatedly. One, platforms must harvest as much data as they can so it can be monetized. Two, platforms must allow just about anything to appear on their platforms to grow traffic. If they stop doing either of these things, their revenues will decline, and stock prices will plummet. Case in point: Facebook’s record loss of \$119 billion in market value over concerns that privacy and security issues will affect profits.

In fact, and not surprisingly, Google created a video that confirmed what we are stating. In the video, Google showcased their true intentions. The [video](#) describes how widespread data collection could be used to shape the decisions society makes. The video explores how, using what it learns, it could shape users’ health and environmental decisions, issues that “reflect Google’s values as an organization.” All the while, Google owns the data a consumer sees while making sensitive and important life decisions.

The Digital Citizens Alliance also made a [video](#) showcasing how the platform business model directly leads to consumer harm, irrespective of who sits at the helm of any of these giant tech companies.

Further, and in order to critically evaluate the true harmful impact of this platform revenue model on consumers, the Digital Citizens Alliance conducted a series of in-depth research projects. These reports are attached for the Commission’s review, and are linked here:

1. Fool Me Once -

[https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DigitalCitizens\\_FoolMeOnce-Final.pdf](https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DigitalCitizens_FoolMeOnce-Final.pdf)

2. Digital Platforms in Crisis: A Decade in the Making –

[https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA\\_Digital\\_Platforms\\_in\\_Crisis.pdf](https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Digital_Platforms_in_Crisis.pdf)

3. The Gateway Trojan –

[https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/2017\\_7The\\_Gateway\\_Trojan.pdf](https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/2017_7The_Gateway_Trojan.pdf)

4. Fear Loathing and Jihad –

<https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/fear-loathing.pdf>

5. Digital Weeds –

<https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/digital-weeds.pdf>

Repeatedly, we saw consumers being directly harmed by a business model that is innately harmful. As such, action is needed now, and we would be honored to provide further information and testimony at the designated hearings to further evaluate these issues.

Sincerely,  
Tom Galvin  
Executive Director  
Digital Citizens Alliance

--

About the Digital Citizens Alliance

Digital Citizens is a consumer-focused group whose mission is to raise awareness among the public and policymakers about how to make the Internet safer.

Digital Citizens engages with key Internet stakeholders - individuals, Internet companies, and civic leaders - to search for solutions to Internet safety issues.

Based in Washington, DC, the Digital Citizens Alliance counts among its supporters the health, pharmaceutical, creative and security industries; online safety experts; and other communities such as consumer advocates focused on Internet safety.

Over the past five years, Digital Citizens has:

- Worked with creative and security industries to raise consumer awareness on the alarming interconnection between hackers and online pirate websites trying to infect computers and other devices.
- Worked with anti-steroids advocates to raise awareness about the ease these drugs are available online, especially among our nation's youth.
- Collaborated with the pharmaceutical industry to encourage citizens to properly dispose of opioids and other prescription drugs.
- Conducted investigations of online pharmacies' willingness to sell prescription painkillers and other drugs to underage teens that don't have a prescription.
- Worked with security experts on the rampant sale of college .edu emails and passwords belonging to faculty, staff and students at colleges across the country.

- Raised concerns about the blurring of the lines between mainstream digital platforms and the so-called Dark Web, including the sale of stolen credit cards, drugs and merchandise.
- Worked with the legal gambling industry on the rise of so-called Internet sweepstakes cafes in states and their efforts to skirt local gambling laws.

We welcome ideas on how to make the Internet a safer place for all citizens.

#### About Tom Galvin

Based in Washington, DC, Tom Galvin has been active on Internet security and safety issues for nearly two decades. As Executive Director of the Digital Citizens Alliance, Tom is focused on raising awareness about issues such as piracy and malware, the illegal online sale of opioids, steroids and other prescription drugs and the blurring of the lines between the Dark Web and mainstream digital platforms.

As an adviser, Tom helped launch [stopbadware.org](http://stopbadware.org), an innovative neighborhood watch program to combat malware; advised the National Cyber Security Alliance on cyber programs; and, guided companies creating national and state Internet security initiatives. Tom also served as Vice President of Government Relations and Communications at VeriSign, where he collaborated with policymakers on homeland security, Internet security and telecommunications issues.

////