

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Expanding Consumers' Video Navigation Choices)	MB Docket No. 16-42
)	
Commercial Availability of Navigation Devices)	CS Docket No. 97-80

COMMENTS OF DIGITAL CITIZENS ALLIANCE

Tom Galvin
Executive Director
Digital Citizens Alliance
1150 17th Street, NW Suite 700
Washington, DC 20036

April 22, 2016

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION AND SUMMARY.....	- 3 -
II. BACKGROUND.	- 4 -
III. THE FCC’S PROPOSALS WOULD FAIL TO PROTECT NAVIGATION DEVICES FROM HACKERS OR DEVICE MALFUNCTION..	- 6 -
IV. THE FCC’S PROPOSALS WOULD ALLOW NEW AND UNIQUELY INVASIVE ADVERTISEMENTS INTO CONSUMERS’ LIVING ROOMS.	- 9 -
V. THE FCC’S PROPOSALS COULD INCREASE CONSUMERS’ EXPOSURE TO HARMFUL MALWARE AND PIRATED CONTENT.....	- 11 -
VI. THE FCC MUST FULLY CONSIDER THESE PRIVACY AND SECURITY RISKS BEFORE EXPANDING ACCESS TO CONSUMERS’ PERSONAL INFORMATION.....	- 12 -
VII. CONCLUSION.....	- 15 -

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Expanding Consumers’ Video Navigation Choices)	MB Docket No. 16-42
)	
Commercial Availability of Navigation Devices)	CS Docket No. 97-80

COMMENTS OF DIGITAL CITIZENS ALLIANCE

Digital Citizens Alliance (“Digital Citizens”) submits these comments in response to the Federal Communications Commission’s (“FCC” or “Commission”) Notice of Proposed Rulemaking (“NPRM”).¹ Digital Citizens applauds the FCC for exploring ways to spur innovation and competition. We are concerned, however, that the FCC’s proposals will have unintended consequences that unnecessarily place consumers’ privacy and security at risk.

I. INTRODUCTION AND SUMMARY.

The FCC’s proposals are problematic for at least three reasons. First, the proposals would allow new and uniquely invasive advertisements to be introduced into consumers’ living rooms. Second, the proposals would fail to protect navigation devices from hackers or device malfunction. Third, the proposals could increase consumers’ exposure to harmful malware and pirated content.

The FCC should consider and address these concerns before it authorizes a new class of potentially harmful and dangerous devices to attach to the nation’s video distribution networks.

¹ *Expanding Consumers’ Video Navigation Choices; Commercial Availability of Navigation Devices*, Notice of Proposed Rulemaking and Memorandum Opinion and Order, 31 FCC Rcd 1544 (2016) (“NPRM”).

Achieving information security and privacy are obviously iterative, life-cycle processes where the job is never truly “done.” But failing to place sufficient emphasis on asset management and risk reduction before authorizing these new technologies threatens the FCC’s ability to fulfill its statutory mandate to “assure the commercial availability . . . of interactive communications equipment” to consumers.² Adopting basic safeguards to protect consumers against harm prior to authorizing an entirely new category of devices will help instill consumer confidence in the reliability and security of over-the-top services and ultimately advance the FCC’s goal of establishing meaningful competitive alternatives to the set-top boxes that multichannel video programmer distributors (“MPVDs”) currently provide to consumers.

II. BACKGROUND.

Digital Citizens is a coalition of consumers, businesses, and Internet experts focused on educating the public and policymakers on the threats people from all walks of life face on the Internet.³ Digital Citizens is based in Washington, D.C. and has a broad range of supporters, including: private citizens; online safety experts; the health, pharmaceutical, creative, and other leading industries; and other communities focused on Internet safety.⁴

Our goal is simple. We want to make the Internet free of: scams and fraud, including identity theft and misleading advertising; dangerous drugs sold online to unsuspecting individuals; and illegal movies, videos, music, images, and other content that steal from citizens and put consumers at risk.⁵

² 47 U.S.C. § 549 (a).

³ See Digital Citizens Alliance, *About the Digital Citizens Alliance*, <http://www.digitalcitizensalliance.org/cac/advocacy/content.aspx?page=about> (last visited Apr. 19, 2016).

⁴ See *id.*

⁵ See *id.*

We have published reports on rogue elements preying on innocent consumers. For example, our research has delivered startling findings on: (1) just how easy it is to buy illegal steroids and prescription drugs online; (2) the extent of counterfeiting internationally; (3) the surprisingly high number (35%) of young adults who report ordering gifts online and not receiving them; (4) the hundreds of millions of dollars content theft sites make each year through advertising alone; and (5) how hackers and malware peddlers are using content theft to bait consumers into unknowingly turning over sensitive financial and personal information.⁶

This research has been featured in reports on ABC World News Tonight, on Good Morning America, in the Washington Post, as well as on local television stations and in newspapers around the country. For example, ABC News featured our research on the black market website Silk Road⁷ in a 2014 story about how this “hidden online haven for drug trafficking” had not only returned, but was more vibrant than ever.⁸ And the Washington Post ran a 2015 story on our research⁹ that found that sites distributing pirated videos were far more likely to expose visitors to dangerous software than legitimate streaming sites or the Internet at large.¹⁰ Consistent with those efforts, we submit these comments to recommend that the FCC

⁶ See Digital Citizens Alliance, *Investigative Reports*, <http://www.digitalcitizensalliance.org/cac/alliance/resources.aspx> (last visited Apr. 19, 2016).

⁷ See Digital Citizens Alliance, *Busted, But Not Broken: the State of Silk Road and the Darknet Marketplaces* (2014), <http://bit.ly/1fzdGNk>.

⁸ See Matthew Mosk, *Underground Website Used for Black Market Sales Bigger Than The Original, Report Says*, ABC NEWS (Apr. 30, 2014), <http://abcnews.go.com/Blotter/silk-road-underground-website-black-market-drug-sales/story?id=23528712>.

⁹ See Digital Citizens Alliance, *Digital Bait: How Content theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Personal Data* (2015), <http://bit.ly/1Uaa3gf> (“Digital Bait”).

¹⁰ See Andrea Peterson, *That Illegal Streaming Site you Love? It May be Infecting You with Malware*, WASHINGTON POST (Dec. 11, 2015), <https://www.washingtonpost.com/news/the-switch/wp/2015/12/11/that-illegal-streaming-site-you-love-it-might-be-infecting-you-with-malware/>.

take meaningful steps to protect consumer expectations of security and privacy prior to authorizing a set of enhanced, interconnected, and potentially vulnerable devices capable of collecting sensitive personal information from everyone in the home, including children.

III. THE FCC’S PROPOSALS WOULD FAIL TO PROTECT NAVIGATION DEVICES FROM HACKERS OR DEVICE MALFUNCTION.

As the Department of Justice and the Federal Trade Commission (“FTC”) recently noted, “[c]yber threats are becoming increasingly more common, more sophisticated, and more dangerous.”¹¹ While the FCC’s NPRM identifies a handful of measures intended to protect MVPDs’ programming content from unauthorized access,¹² the FCC does not propose to adopt any measures to protect navigation device hardware or software from unauthorized access obtained through hacking or device malfunction. It should.

Navigation devices have access to sensitive personal information that can give hackers a look into our living rooms and our lives. For example, these devices have access to information about our preferred television programs, our consumption patterns, and our recent searches. In addition, when connected to a smart television or other advanced device, navigation devices could be used to record and transmit audio, video, or images – literally becoming “eyes” and “ears” in consumers’ living rooms.

The risk that hackers would be able to use navigation devices to obtain access to sensitive personal information is high. Most navigation devices will likely be low-cost consumer-grade

¹¹ Department of Justice and Federal Trade Commission, *Antitrust Policy Statement of Sharing Cybersecurity Information*, <http://1.usa.gov/241hHPI> (last visited Apr. 20, 2016).

¹² See NPRM ¶¶ 50-62. Although not the focus of our comments, the FCC’s proposals are likely woefully inadequate to protect against content theft. Many have already spoken up about this issue. For example, Walking Dead producer Gale Anne Hurd calls them a “disaster for those of us who are trying to figure out how to keep making the movies and TV shows audiences love.” Gale Anne Hurd, *Stop Piracy Apocalypse*, USA TODAY (Apr. 12, 2016), <http://usat.ly/1VjOAW8>.

products that can be easily manipulated by hackers, their owners, or other unauthorized third-parties. Unlike computers, moreover, consumers cannot protect their navigation devices with antivirus software because none currently exists for such devices.¹³ Indeed, like the smart televisions they connect to, navigation devices are “always on,” “vulnerable,” and “waiting to be attacked.”¹⁴ Just ask Vizio, which recently learned that its devices’ storage of viewing data was vulnerable to “digital eavesdropping” and had been intercepted by a hacker.¹⁵

The current generations of navigation devices are less vulnerable to hacking in part because contractual agreements between their manufacturers and MVPDs require hardening the devices against unauthorized access.¹⁶ The use of non-standard, proprietary software by current-generation devices – as opposed to a common, open-sourced platform as the FCC has proposed – also helps guard against vulnerabilities. While current-generation navigation devices are by no means invulnerable to threats, the FCC’s proposal for introducing next-generation devices would increase the risks consumers face. The FCC proposes to sever the contractual safeguards on devices that exist between MVPDs and their set-top box manufacturers while expanding the target for threats onto a common, open-source platform. The FCC should fully consider the risks these actions create before adopting new rules.¹⁷

¹³ See, e.g., Herb Weisbaum, *Smart TVs an “Inevitable” Path to Attach Home PCs*, NBC NEWS (Jan. 19, 2016), <http://www.nbcnews.com/business/consumer/smart-tvs-inevitable-path-hackers-attack-home-pcs-experts-n499611> (noting the lack of security software for televisions and other consumer devices).

¹⁴ See Jeremy Kirk, *The Next Wave of Cybercrime Will Come Through Your Smart TV*, PC WORLD (Dec. 28, 2015), <http://www.pcworld.com/article/3018632/security/the-next-wave-of-cybercrime-will-come-through-your-smart-tv.html>.

¹⁵ See, e.g., Annie Dike, *Smart TVs and Data Privacy Concerns*, THE NATIONAL LAW REVIEW (Feb. 17, 2016), <http://www.natlawreview.com/article/smart-tvs-and-data-privacy-concerns>.

¹⁶ See, e.g., NPRM ¶¶ 16-17.

¹⁷ Communities of hackers have already started to target connected home devices. See, e.g., The IoT Village, *About*, <https://www.iotvillage.org/> (last visited Apr. 21, 2016) (describing workshops, live talks, and contests on hacking off-the-shelf devices).

The consequences of unauthorized access can prove catastrophic. For example, Digital Citizens' 2015 report "Selling 'Slaving,'" which is attached as Appendix A, demonstrated how hackers have hijacked and activated the cameras on young girls' computers to videotape them without their knowledge.¹⁸ These videos are then marketed on websites such as YouTube or used to extort the girls for more material.¹⁹ Cassidy Wolf, a former Miss Teen USA, experienced this exploitation first hand. Her computer was "slaved" by a hacker who used it to take pictures of her changing clothes and listen to her conversations.²⁰ The hacker then used this data to attempt to extort Cassidy into providing even more material – for instance, videos of her doing what he asked and "better quality" photos.²¹

The navigation devices under consideration in this proceeding would not even need to be hacked to create these types of problems. Device malfunctions or programming errors could cause them to collect and share sensitive personal information.²² For example, in 2013, smart televisions manufactured by LG Electronics ("LG") were caught collecting and transmitting data on consumers' viewing habits even after they had activated a privacy setting designed to prevent this from happening.²³ LG apologized to its customers and admitted that the sets were "behaving

¹⁸ See Digital Citizens Alliance, *Selling "Slaving": Outing the Principal Enables that Profit from Pushing Malware and Put Your Privacy at Risk* (2015), <http://bit.ly/1UmQB2k>.

¹⁹ See *id.*

²⁰ See *id.* at 10-12.

²¹ See *id.*; see also David Bisson, *Attackers Using RATs to "Slave" Victims' Computers, Sextort Children*, State of Security (Aug. 5, 2015), <http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/attackers-using-rats-to-slave-victims-computers-sextort-children/>.

²² See, e.g., Gary Davis, *LG Smart TVs Leak Data Without Permission*, MCAFEE CONSUMER BLOG (Dec. 2, 2013), <https://blogs.mcafee.com/consumer/lg-smart-tvs-leak-data/>.

²³ See Jane Wakefield, *LG Promises Update for "Spying" Smart TV*, BBC NEWS (Nov. 21, 2013), <http://www.bbc.com/news/technology-25042563>.

in ways they shouldn't be."²⁴ However, as professor Dan Wallach of Princeton University emphasized after the LG incident, the deeper issue is that that "it's relatively easy to build something that works, but it's significantly harder to build something that's secure and respects privacy."²⁵ For these reasons, the FCC must be vigilant in ensuring that navigation devices respect consumer privacy and protect consumer security.

IV. THE FCC'S PROPOSALS WOULD ALLOW NEW AND UNIQUELY INVASIVE ADVERTISEMENTS INTO CONSUMERS' LIVING ROOMS.

The FCC's proposals will likely upset consumers' settled expectations about which of their family's media consumption habits are private and which are public. To take just one example, the FCC's proposals would likely allow set-top box vendors to use consumer Internet searches and browsing histories to inform the types of advertising that appears during television shows. Imagine, for instance, if a married couple started to receive television advertisements for divorce attorneys or online dating websites based on one of the spouse's Internet browsing histories. Or if a child was exposed to television advertisements about divorce, terminal illness, or other sensitive topics that one of her parents may have recently researched.

These kinds of unintended consequences are especially problematic because they are so sharply at odds with consumer expectations of how television works. Although consumers have grown to expect that Internet sites will provide ads based on our recent searches or browsing history, they view their televisions differently. Computers and smartphones are very personal devices that consumers frequently use to search for things they may not want others to see. We

²⁴ See *id.*; Matt Bryan, *LG Promises to Stop Your Smart TV Spying On You*, ENGADGET (Nov. 21, 2013), <http://www.engadget.com/2013/11/21/lg-admits-smart-tv-data-collection/>.

²⁵ See Charles Arthur, *Information Commissioner Investigates LG Snooping Smart TV Data Collection*, THE GUARDIAN (Nov. 21, 2013), <https://www.theguardian.com/technology/2013/nov/21/information-commissioner-investigates-lg-snooping-smart-tv-data-collection>.

may not like receiving advertisements based on web searches conducted by PC, tablet, or phone, but we expect some measure of monitoring and have learned to avoid it or at least tolerate it. In contrast, televisions offer communal experiences that we share with friends and family – often in our homes' living rooms, dens, kitchens, or other gathering spots.

Digital Citizens' recent polling confirms that most Americans recognize the distinction between personal electronic devices and communal viewing experiences. Our analysis highlights the seriousness of potentially blending computer/smartphone activity with the television advertising that airs in our living rooms. We polled 685 American adults with varying geographic and economic backgrounds on April 13 and 14, 2016 using a Vрге Analytics poll.²⁶ Among other things, we found that 66 percent of Americans currently recognize the distinction between watching television in their living room (a communal experience) and using their computers and smartphones (a personal experience).²⁷ We also found that 73 percent of Americans would be bothered if advertisements related to their online browsing activity appeared while they were watching television in their living rooms with family or friends.²⁸ The FCC's approach toward authorizing competitive navigation devices needs to remain attentive to the vast gulf in consumer expectations that exist between personal electronic devices and communal viewing systems in the home.

²⁶ See Digital Citizens Alliance, *Americans Fear Privacy Intrusion from FCC Set-Top Box Proposal, According to New Survey* (Apr. 20, 2016), <http://prn.to/1VGK8By>. The poll had a 2.8 percent margin of error.

²⁷ *See id.*

²⁸ *See id.*

V. THE FCC’S PROPOSALS COULD INCREASE CONSUMERS’ EXPOSURE TO HARMFUL MALWARE AND PIRATED CONTENT.

As currently drafted, the FCC’s proposals could make it easier for hackers and malware purveyors to trick consumers into turning over sensitive financial and personal information. For example, assume that a navigation device provides a consumer with three options to watch her desired television program under the FCC’s proposed regime. The first option offers new episodes for \$4 each. The second option offers episodes from previous seasons for \$2 each. And the third option offers all episodes of the show for free via an overseas pirate site.²⁹ Many consumers may select the third option at least some of the time.

What these consumers probably would fail to realize, however, is that piracy is often a doorway to harmful malware that can lead to identity theft, financial loss, and computers being taken over by hackers.³⁰ In fact, the cyber security firm RiskIQ recently found that one out of every three piracy sites contains malware.³¹ It also found that consumers are 28 times more likely to get malware from a piracy site than a mainstream website or licensed content provider.³² Just as worrisome, merely visiting this type of site can place users’ devices at risk – 45 percent of this malware was delivered through “drive-by downloads” that invisibly downloaded to the users’ computers without requiring them to click a link.³³ Under the FCC’s current proposals, malicious threats such as these will be far more able to target navigation devices and proliferate in consumers’ homes.

²⁹ *See Digital Bait* at 17.

³⁰ *See id.* at 1.

³¹ *See id.*

³² *See id.*

³³ *See id.*

VI. THE FCC MUST FULLY CONSIDER THESE PRIVACY AND SECURITY RISKS BEFORE EXPANDING ACCESS TO CONSUMERS' PERSONAL INFORMATION.

The FCC deserves credit for its efforts to promote innovation and competition in the marketplace for navigation devices.³⁴ However, the FCC must proceed deliberately and cautiously given the important privacy interests that are at stake.³⁵ In particular, the FCC should expand access to consumers' information only after it has taken affirmative measures to safeguard consumer security and privacy.

At the very least, the FCC should fully consider and quantify the privacy risks that its proposals pose. For example, we can only speculate as to the total reach – and annual cost to U.S. consumers – of hacking tactics such as botnets, distributed denial-of-service attacks, spamming and phishing, and distributed financial fraud.³⁶ Even the FCC has limited experience with these new types of threats and the risks that they pose, which further underscores the need for additional inquiry to fully appreciate them.

Once the FCC better understands and fully considers these risks, it should take additional steps to ensure that navigation devices will not be used to spy on their owners or disrupt the communal experience offered by watching television at home with family and friends. These steps may include addressing potential technological issues, such as how to ensure that navigation devices are both secure and reliable, along with those related to the FCC's authority to act in this sphere.³⁷

³⁴ See, e.g., NPRM ¶¶ 1-3.

³⁵ See, e.g., *id.* ¶ 73

³⁶ See, e.g., *Digital Bait* at 1, 14 (noting a recent “significant change” in content thieves' business models).

³⁷ See, e.g., NPRM ¶¶ 21-24.

Consistent with the launch of any new systems architecture, the FCC’s pre-authorization risk-management program might follow the basic, four-part model of (1) assessment, (2) design, (3) implementation and (4) operation. Within the risk-assessment phase, vendors should be asked to identify a security policy, evaluate their ability to identify and remediate vulnerabilities, and document their ability to conduct iterative risk assessments. Within the product-design phase, the vendors should be required to identify and rate risks and then design the system architecture that is informed both by the risks identified during the assessment phase and the ordering of those risks by the vendor. Within the implementation phase, vendors should apply security controls and implement robust testing in a secure environment or “sandbox” prior to commercial operation. Finally in the operation phase, vendors should be responsible for ongoing security as well as intrusion detection and response.

The FCC could use its equipment authorization process as a model.³⁸ For example, just as the FCC does not allow certain devices to be sold or marketed in the United States until they demonstrate compliance with its radiofrequency (“RF”) standards,³⁹ it should not allow navigation devices to be sold or marketed in the United States without cybersecurity approval. Third-party bodies, or even the FCC’s Telecommunications Advisory Council (“TAC”),⁴⁰ could establish standards for device designers and manufacturers to follow, and the FCC could affirm through equipment authorization or certification processes that these standards are observed.

³⁸ See, e.g., FCC, *Equipment Authorization Approval Guide*, <https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization> (last visited Apr. 20, 2016).

³⁹ See, e.g., FCC, *Wireless Devices and Health Concerns*, <https://www.fcc.gov/consumers/guides/wireless-devices-and-health-concerns> (last visited Apr. 20, 2016)

⁴⁰ See, e.g., TAC Cybersecurity Working Group, Applying Security to Consumer IoT Devices Subcommittee, *Technical Considerations White Paper* (Dec. 2015), <https://transition.fcc.gov/oet/tac/tacdocs/reports/2015/FCC-TAC-Cyber-IoT-White-Paper-Rel1.1-2015.pdf>.

The FCC has moved in this direction in other contexts by, for instance, requiring white space devices to “incorporate adequate security measures.”⁴¹ In the case of nearly ubiquitous television navigation device, the risk of consumer harm is great enough to go somewhat further by identifying a baseline for precisely which security measures are “adequate” and by ensuring that basic security measures are incorporated into navigation devices prior to introducing these devices into the stream of commerce.

The patchwork quilt of Federal and state enforcement of analogous rules and state-specific privacy protections that the FCC has proposed to rely on falls far short of the holistic approach to cybersecurity seen in other important sectors of the United States economy.⁴² The most comprehensive consumer protection regime likely comes from the FTC, which relies on its authority to halt unfair or deceptive acts or practices to protect consumers against cyber threats.⁴³ But after-the-fact enforcement by the FTC remains a poor substitute for sensible planning for readily predictable threats. Indeed, the cybersecurity best practices for products as diverse as aviation, automobiles and banking uniformly emphasize focusing on risk reduction *before* the deployment of technology.⁴⁴ Focusing on identifying the risks that novel set-top navigation devices pose to consumers and insisting on intelligent design from the outset will allow end-

⁴¹ See, e.g., 47 C.F.R. §§ 15.709(f), 15.711(j).

⁴² See, e.g., NPRM ¶¶ 77-78 (asserting that navigation device developers “must already ensure that their products and services meet the privacy standards of the strictest state regulatory regime” and seeking comment on the scope of state privacy laws).

⁴³ 15 U.S.C. § 45. The FTC also has data security enforcement authority under the Gramm-Leach-Bliley Act and the Safeguards Rule, Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, the Health Information Technology for Economic and Clinical Health Act, and the Children’s Online Privacy Protection Act and its implementing rule. See, e.g., FTC Commissioner Julie Brill, *Stepping into the Fray: The Role of Independent Agencies in Cybersecurity*, Keynote Address (Sept. 17, 2014), <http://1.usa.gov/1V12eZg>.

⁴⁴ See National Highway Traffic Safety Administration, *A Summary of Cybersecurity Best Practices* (2014), <http://bit.ly/1TjxzYJ>.

users to select the right product and, ultimately, accelerate the deployment of competitive navigation devices to the public.

VII. CONCLUSION.

The FCC's proposed framework for navigation devices may have the potential to drive greater competition and innovation, but cybersecurity and privacy concerns currently outweigh any potential benefits. The FCC's proposals also threaten to undo progress toward a more competitive set-top box environment. Before the FCC opens new avenues for cyber-attacks and violations of privacy for intensely sensitive consumer data, the FCC should adopt a comprehensive method of ensuring ensure that newly authorized navigation devices are designed to a level of security consumers would expect of a product in what will become a highly integrated new video-collection and distribution ecosystem. The FCC should fully consider and address these concerns prior to authorizing new navigation devices to ensure that the potential benefits of its proposals are not undone or outweighed by the public harms associated with expanding access to sensitive consumer information.

Respectfully submitted,

By: /s/ Tom Galvin

Tom Galvin
Executive Director
Digital Citizens Alliance
1150 17th Street, NW Suite 700
Washington, DC 20036

April 22, 2016