

June 8, 2016

The Honorable Thomas Wheeler
Chairman
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Chairman Wheeler:

We write today to express security-related concerns with your “set-top box proceeding” (NPRM MB Docket No. 16-42). Your proposal to allow access of third-party device manufacturers and software developers into cable, satellite, and telco TV providers’ existing networks and servers requires American consumers, creators, and providers to “trust” these third-parties, without a workable security and enforcement regime. As the global economy continues to push the limits of security in unprecedented ways, we must be vigilant in assessing all potential vulnerabilities, including those proposed by the Federal Communications Commission (FCC).

Cybersecurity, supply chain management, data security and privacy have been the topics of numerous hearings and legislation due to the threats to individual consumers, critical infrastructure, and our national and economic security. In addition, this Administration has made cybersecurity a key focus from the development of the NIST Cybersecurity Framework to the efforts of the Intelligence Community and the Department of Homeland Security. The FCC has been deeply involved in public safety and cybersecurity issues. That is why we are surprised and concerned about this latest proceeding and the risks it would create by opening up access into our homes and our networks, with little government oversight.

The FCC proposes to require multichannel video programming distributors (MVPDs) to make three “flows” of information available to “manufacturers, retailers, and other companies that are not affiliated with an MVPD.”¹ While the FCC suggests the possibility of a limited “robustness” requirement, the proposal would allow device makers to circumvent direct contractual, licensing and technical protections, and instead, to ‘self-certify’ the lawfulness of their actions without any effective mechanism for detection or enforcement. Self-certification would permit third parties to reach network entitlement servers, billing, and local, regional and national content servers. In fact, under the item “MVPDs cannot withhold the three Information Flows if they have received such certification and do not have a good faith reason to doubt its validity.”²

¹ Fed. Comm’n Comm’n, MB Docket 16-42, CS Docket 97-80, Notice of Proposed Rulemaking and Memorandum Opinion and Order, para. 2 (Feb. 18, 2016).

² *Id.*

Not only are network owners limited in their ability to establish direct security controls, the proposed rule further undermines security by limiting MVPD access to information that might be necessary to detect bad actors. The FCC proposal provides no technical means for monitoring device or company behavior and requires that competitive retail devices must “have no business relationship with any MVPD.”³ Since the FCC has no authority to monitor or compel compliance with the self-certifications, this truly allows the fox to guard the hen house. Furthermore, existing statutory security and privacy requirements applicable to MVPDs under the Communications Act do not apply to device and software manufacturers.

In addition, there is minimal discussion in the item addressing potential risks that might arise if third-party apps and Internet-connected devices accessing MVPD services create new avenues of intrusion into network infrastructure and Internet-connected consumer devices. There is a lack of appreciation for the ways in which self-certified devices and captured viewing data might facilitate the illegal activities of cybercriminals in selling pirated content or promoting other illegal activity. For example, a December study by Digital Citizens Alliance estimates that sites trafficking in pirated content collect \$70 million per year for installing malware, not just offering pirated content. The FCC must not adopt final rules until these security concerns are thoroughly vetted and addressed.

While we certainly hope that reputable manufacturers from the United States would protect consumer information, copyrights, and our networks from harm, there is no guarantee manufacturers from other nations would have the same incentive to do so. Our previous experience makes us extremely suspicious.

We are concerned that the FCC’s set-top box proceeding potentially provides cyber criminals access into homes or property without adequate protections, oversight, or enforcement. In order for us to understand how the FCC intends to ensure the set-top box proceeding protects the security of consumers’ information, high-value content, and the nation’s critical infrastructure, please provide answers to the following questions no later than June 30, 2016:

1a. Has the FCC considered the security implications of its set-top box proposal? If yes, please specify, particularly in relation to malware and pirated content. As adopted, the NPRM does not address this issue.

b. Has the FCC assessed the potential economic impact on U.S. consumers based on increased potential of identity theft? Has the FCC assessed the potential economic impact on U.S. copyright owners/creators due to potential theft? Has the FCC assessed the potential damage to other U.S. businesses, including critical infrastructure and the loss of trade secrets, which may be impacted through security breaches resulting from malware or other harms resulting from the “flow” path? If yes, please specify.

2.a. Can the FCC impose security and privacy requirements on manufacturers and software developers? If yes, under what statutory authority?


³ See, e.g., Notice of Proposed Rulemaking at ¶23.

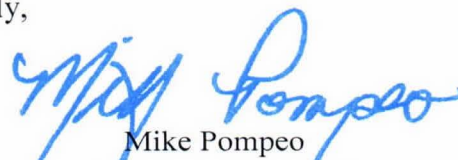
- b. What security and privacy requirements will apply to manufacturers and software developers – Sections 338(i) and 631 of the Communications Act, or other requirements?
3. Will the FCC independently evaluate whether manufacturers and software developers' self-certifications are valid?
4. Will the FCC use audits or some other investigative means to evaluate whether manufacturers and software developers are complying with U.S. privacy and security requirements?
5. If a manufacturer or software developer is determined by the FCC not to be in compliance with U.S. security and privacy requirements, what specific actions will the FCC take? In particular, will the FCC revoke an entity's certification and prohibit MVPDs from providing the information flow?
6. If a manufacturer or software developer is determined by the FCC not to be in compliance with U.S. security and privacy requirements, will such entity be permitted to remedy its non-compliance, or will it be permanently precluded from receiving the information flows?
- 7.a. How will the FCC determine whether a foreign manufacturer or software developer has transferred U.S. consumer, business or government information outside of the U.S.?
- b. How will the FCC determine whether such manufacturer or software developer has transferred U.S. consumer, business or government information to another foreign entity?
8. If a foreign manufacturer or software developer has inappropriately transferred U.S. consumer, business, or government information outside of the U.S., what steps will the FCC take to compel the manufacturer or software developer to delete the information?
8. If a foreign manufacturer or software developer has transferred U.S. consumer, business or government information outside of the U.S., what legal recourse would the FCC have to stop the foreign entity from using or sharing the information?

Based upon these open security questions, we remind you of the statutory prohibition in section 629 of the Communications Act that prohibits the FCC from jeopardizing the security of MVPD services and your mandate to protect the public interest.

Thank you for providing responses to these questions in a timely manner. Please contact Geoffrey Kahn at 202-226-1770 and Walter Gonzalez at 202-225-3061 if you have any questions.

Sincerely,


Devin Nunes
Member of Congress


Mike Pompeo
Member of Congress