

June 8, 2016

The Honorable Thomas Wheeler  
Chairman  
Federal Communications Commission  
445 12<sup>th</sup> 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.”<sup>1</sup> 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.”<sup>2</sup>

---

<sup>1</sup> 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).

<sup>2</sup> *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.”<sup>3</sup> 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?

---

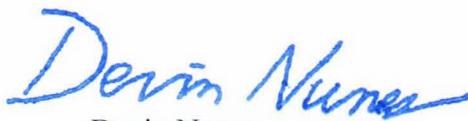
<sup>3</sup> See, e.g., Notice of Proposed Rulemaking at ¶23.

- 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?

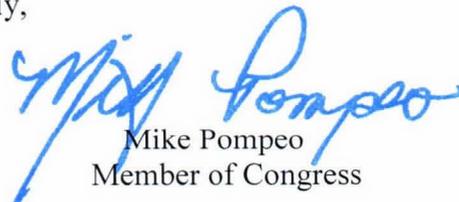
Based upon these open security questions, we remind you of the statutory prohibition in section 629 of the Communications Act that prohibits the FCC from jeopardizing the security of MVPD services and your mandate to protect the public interest.

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



FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

OFFICE OF  
THE CHAIRMAN

July 11, 2016

The Honorable Devin Nunes  
U.S. House of Representatives  
1013 Longworth House Office Building  
Washington, D.C. 20515

Dear Congressman Nunes:

Thank you very much for sharing your questions about how the Commission's proceeding for better fostering competition in the set-top box and navigation app marketplace might impact security and privacy issues. I take your input on these issues seriously and assure you that it will receive careful consideration.

Protecting the nation's networks is a top priority for the FCC. Commission personnel work around the clock—including in a 24/7 operations center—to safeguard America's telephone, radio, cable, satellite, and Internet connectivity. The Commission takes our security responsibilities very seriously, and we leverage extensive staff expertise to ensure our policy proposals accord with best practices and the best available science.

We bring this cybersecurity experience and awareness to all of the rulemakings we undertake to fulfill our responsibilities under the Communications Act, including our current efforts to update our rules implementing section 629 of the Act. Section 629 of the Communications Act, adopted by Congress in 1996, requires the Commission to promote competition in the market for devices that consumers use to access their pay-television content. Yet, unfortunately, the statutory mandate in section 629 is not yet fulfilled. The lack of competition in this market has meant few choices and high prices for consumers. In a recent Rasmussen Report Study, 84 percent of consumers felt their cable bill was too high. One of the main contributing factors to these high prices is the no-option, add-on fee for set-top box rental that is included on every bill, forcing consumers to spend, on average, \$231 in rental fees annually. Even worse, a recent congressional investigation found that the price of most equipment fees is determined by what the market will bear, and not the actual cost of the equipment.<sup>1</sup> With the lack of competition in this market, it should come as little surprise that fees for set-top boxes continue to rise.<sup>2</sup> Clearly, consumers deserve better.

This February the Commission put out for public comment a proposal that would fulfill the statutory requirement of competitive choice for consumers. This action opened a fact-finding

---

<sup>1</sup> U.S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS COMMITTEE, MINORITY STAFF REPORT, INSIDE THE BOX: CUSTOMER SERVICE AND BILLING PRACTICES IN THE CABLE AND SATELLITE INDUSTRY, 17 (Jun. 23, 2016).

<sup>2</sup> One recent analysis found that the cost of cable set-top boxes has risen 185 percent since 1994 while the cost of computers, television and mobile phones has dropped by 90 percent during that same time period.

dialog to build a record upon which to base any final decisions. Our record already contains more than 280,000 filings, the overwhelming majority of which come from individual consumers. My staff is actively engaged in constructive conversations with all stakeholders—content creators, minority and independent programmers, public interest and consumer groups, device manufacturers and app developers, software security developers, and pay-TV providers of all sizes—on how to ensure that consumers have the competition and choice they deserve. I am hopeful that these discussions will yield straightforward, feasible, and effective rules for all.

You raise questions about how this proceeding might affect the network security protections currently in place. The Notice of Proposed Rulemaking (NPRM) adopted in February proposes a careful balance between network security and section 629's mandate that consumers be able to enjoy pay-television content with the equipment of their choice. Cable and satellite providers would be required to support a narrow, defined set of interfaces that would allow competitive devices and apps to access television content. These types of interfaces, usually termed Application Programming Interfaces (APIs), are routinely offered by online services. APIs allow a third party (such as a competitive navigation device provider) to interface with an organization's systems, without revealing any internal design, operation, or data about the organization. Third parties that connect to an API are not granted full system access, and are limited to only the features provided by the API. Securing an API is easier than securing internal systems, because an API only has to support specific functionality. Best practices for API security are readily available and widely practiced.<sup>3</sup>

The NPRM proposal would bring to television services the same secure modularity that phone and Internet customers have long enjoyed. In the telephone context, for example, a user can purchase and operate a third-party (e.g. Samsung) phone; the phone is not granted full access to telephone carrier (e.g. Verizon) internal systems. Similarly, in the Internet context, a user can purchase and operate a third-party (e.g. Arris) modem; that modem is not granted full access to the Internet Service Provider's (e.g. Comcast) internal systems.

All of the major cable and satellite providers, in fact, already support APIs for authenticating user credentials—some of the most sensitive information in the television ecosystem. Services like HBO Go<sup>4</sup> and Showtime Anytime<sup>5</sup> ensure that customers have subscribed by interfacing with cable and satellite account management systems. These APIs have been supported for over 5 years.

Further, the FCC's set-top box proposal will protect the role of digital rights management (DRM) platforms in the television ecosystem. DRM platforms offer rigorous protection against

---

<sup>3</sup> See, e.g., *OWASP Enterprise Security API Project*, OPEN WEB APPLICATION SOC'Y PROJECT [https://www.owasp.org/index.php/Project\\_Information:\\_OWASP\\_Enterprise\\_Security\\_API\\_Project](https://www.owasp.org/index.php/Project_Information:_OWASP_Enterprise_Security_API_Project) (last visited June 2, 2016).

<sup>4</sup> HBO GO, <http://play.hbogo.com> (last visited June 2, 2016).

<sup>5</sup> SHOWTIME ANYTIME, <http://www.showtimeanytime.com> (last visited June 2, 2016).

unauthorized copying and other violations of content owner rights.<sup>6</sup> Under the FCC's proposal, content owners would remain free to select the DRM platforms that they prefer. Developers of competitive set-top boxes and apps would license the DRM technology and satisfy compliance requirements – in the very same way that current set-top boxes support DRM, and the same way that competitive devices and apps already support DRM for online video. Furthermore, all of the major DRM platforms support revoking authorization for content; if a competitive device or app were ever found to be violating DRM requirements, access to content could be immediately terminated.

You also raise questions about how this proceeding might affect the privacy protections afforded to subscribers of pay-TV. As you know, pay-TV providers are obligated to comply with the privacy obligations imposed by Sections 631 and 338 of the Communications Act. These privacy obligations, among other things, prohibit pay-TV providers from disclosing personally identifiable information concerning any subscriber, including data about a subscriber's viewing habits, without the subscriber's prior consent.

I strongly believe that third-party app developers and device manufacturers must afford consumers the same level of protection as afforded by pay-TV providers. While the NPRM proposes that competitive devices and apps certify compliance with the privacy protections in the Act, we also invited parties to provide alternative proposals that would ensure the preservation of these important privacy protections.

We will continue to engage with stakeholders on this important issue. Notably, our record includes filings on this issue from the Federal Trade Commission (FTC) and a group of state attorneys general (state AGs)—representing the states of California, Illinois, New York, Connecticut, Iowa, Maine, Maryland, Massachusetts, Minnesota, Mississippi, New Jersey, Oregon, Pennsylvania, Vermont, and the District of Columbia. In their comments, the FTC and the state AGs explain that—if we require competitive devices and apps to publicly commit to providing the same privacy protections required of pay-TV providers under the Communications Act—the FTC and the state AGs would be willing and able to enforce the privacy commitments made by third-party app and device manufacturers just as they currently enforce other privacy commitments made by apps and devices. I am confident that by working with stakeholders and our federal and state partners, we will identify clear rules of the road that will afford consumers with strong privacy protections and the enforcement mechanisms necessary to ensure compliance by third parties.

Please find below answers to the specific questions in your letter.

*1a. Has the FCC considered the security implication 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.*

---

<sup>6</sup> See DOWNLOADABLE SEC. TECH. ADVISORY COMM., DSTAC FINAL REPORT 262-67 (Aug. 28, 2015), <https://transition.fcc.gov/dstac/dstac-report-final-08282015.pdf> [hereinafter DSTAC FINAL REPORT].

The NPRM was prompted in part by a congressional directive within the STELA Reauthorization Act of 2014.<sup>7</sup> Section 106(d) of that legislation required FCC to assemble a working group of technical experts to evaluate and recommend options for enhancing downloadable security systems designed to promote the competitive availability of navigation devices. The FCC promptly implemented Congress's directive by chartering the Downloadable Security Technology Advisory Committee (DSTAC) on December 5, 2014.

This DSTAC's membership consisted of diverse technical experts, drawn from content creators, cable and satellite providers, consumer electronics manufacturers, software vendors, public interest organizations, and academia.<sup>8</sup> The group first convened on February 23, 2015. After weekly conference calls and additional in-person meetings, the committee issued its final 344-page report on August 28, 2015.<sup>9</sup> The FCC also received over 100 comments and other submissions in association with this process.<sup>10</sup> You can find this report and other DSTAC materials at: <https://www.fcc.gov/about-fcc/advisory-committees/general/downloadable-security-technology-advisory-committee>.

The DSTAC's participants and commenters provided valuable technical guidance to the Commission, with particular emphasis on security and privacy matters. Over 100 pages of the committee's final report expressly address cable and satellite network security, protecting content, or safeguarding consumer data.<sup>11</sup> Many comments and submissions also addressed security issues.

In addition, as addressed above, the NPRM proposes to secure access to networks through the use of APIs. Third parties that connect to an API are not granted full system access, and are limited to only the features provided by the API. Securing an API is easier than securing internal systems, because an API only has to support specific functionality. In this way, the NPRM proposal would bring to television services the same secure modularity that phone and Internet customers have long enjoyed, without increasing malware risks for network operators.

Further, as also addressed above, the FCC's proposal will ensure that anti-piracy protections remain in place. Our proceeding will protect the role of DRM platforms in the television ecosystem. The NPRM proposed that content owners would remain free to select the DRM platforms that they prefer. Developers of competitive apps and set-top boxes would license the DRM technology and satisfy compliance requirements – in the very same way that current set-top boxes support DRM, and the same way that competitive apps and devices and already support DRM for online video.

---

<sup>7</sup> STELA Reauthorization Act of 2014, Pub. L. No. 113-200, § 106(d), 128 Stat. 2059 (2014)

<sup>8</sup> *Appointment of Members to the Downloadable Security Technology Advisory Committee*, 30 FCC Rcd 389 (Jan. 27, 2015).

<sup>9</sup> DSTAC FINAL REPORT, *supra* note 9.

<sup>10</sup> See MB Docket No. 15-64.

<sup>11</sup> See DSTAC FINAL REPORT, *supra* note 9, at 3-4, 12-16, 24-26, 28-30, 31-37, 47-56, 60-135, 186-192.

In sum, the FCC solicited and benefited from a wealth of security expertise while developing the proposed rulemaking, and we carefully evaluated the input that we received. The Notice of Proposed Rulemaking seeks additional input from stakeholders on the security aspects of the Commission's proposal.<sup>12</sup> The Commission will not take any actions that would increase network vulnerabilities or reduce anti-piracy protections.

*1b. Has the FCC assessed the potential economic impact of 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 specific.*

In light of our comprehensive approach to security issues, our proposal does not increase the risk of identity theft to consumers or the risk of economic harm as a result of security breaches to copyright owners/creators or businesses. As addressed herein and consistent with our duty under section 629(b) to protect system security and sections 631 and 338 to protect subscriber privacy, our proposal protects the integrity of television delivery systems and the rights of content owners. Consumers will have the very same legal remedies available to them today to pursue individuals engaged in identify theft, and content creators will have the very same legal remedies available to them today to pursue individuals who pirate content<sup>13</sup> or circumvent copy protections.<sup>14</sup> Similarly, our proposal would not affect the legal remedies available to U.S. businesses to pursue hackers.<sup>15</sup>

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

*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?*

The Communications Act and Commission rules guarantee a set of public interest protections for current cable and satellite set-top subscribers.<sup>16</sup> These features include strong security and privacy protections, Emergency Alert System messaging, closed captioning, parental controls, and limits on advertising to children. If a cable or satellite provider fails to satisfy these requirements, the Commission is able to ensure corrective measures by initiating an enforcement action.<sup>17</sup>

---

<sup>12</sup> Expanding Consumers' Video Navigation Choices, Notice of Proposed Rulemaking, 31 FCC Rcd 1544, 1568-74, 1576-83, ¶¶ 50-62, 70-80.

<sup>13</sup> *E.g.*, 47 U.S.C. §§ 501-506 (civil cause of action and criminal penalties for copyright infringement).

<sup>14</sup> *E.g.*, 17 U.S.C. § 1201 (civil cause of action and criminal penalties for circumventing content protections).

<sup>15</sup> *E.g.*, 18 U.S.C. § 1030 (civil cause of action and criminal penalties for computer trespass).

<sup>16</sup> Expanding Consumers' Video Navigation Choices, *supra* note 12, 1579-80, ¶ 73.

<sup>17</sup> *E.g.*, Cox Communications, Inc. Order and Consent Decree, 30 FCC Rcd. 12302 (Nov. 5, 2015) (enforcement action against a cable provider that did not adequately secure customer information).

The NPRM seeks to ensure that these important and longstanding public interest features continue to be guaranteed in competitive set-top boxes and video apps that access cable and satellite content. We propose accomplishing this goal through a certification process, in which third-party devices' and apps' interoperability with cable and satellite networks will be conditioned on the devices' and apps' compliance with these public interest features.

The Federal Trade Commission, state attorneys general, and private litigants are generally able to pursue businesses that misrepresent their security and privacy practices. We anticipate that we and our partners at FTC would vigorously protect public interest features in competitive devices and apps, in much the same way that FCC already protects those same features in cable and satellite devices and apps. The NPRM seeks comment on these certification and enforcement mechanisms.

*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?*

Response to Questions 3 & 4:

A business that offers a competitive set-top box or video app that accesses cable and satellite content would commit to adopting reasonable security safeguards and privacy safeguards consistent with Sections 338 and 631 of the Act. The purpose of this certification is to ensure a clear set of rules and strong enforcement authority. The NPRM seeks comment on the best certification process, whether certification to consumers, certification to cable and satellite providers, certification to the Commission, or certification to an independent body to ensure compliance. If a device manufacturer or software vendor failed to implement adequate precautions, it would risk enforcement action under the Federal Trade Commission Act and similar state statutes. Cable and satellite providers could also revoke interoperability with that set-top box or video app.

Under the proposal set forth in the NPRM, a competitive device or app could also be subject to technical auditing for ensuring adequate content protection. The NPRM's proposal would not alter the current landscape of DRM platforms, some of which require technical validation for a device or app to be compliant.<sup>18</sup> The NPRM seeks comment on whether independent testing should be required for other navigation device security properties.<sup>19</sup>

*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*

---

<sup>18</sup> Expanding Consumers' Video Navigation Choices, *supra* note 1, ¶ 71.

<sup>19</sup> *Id.* ¶¶ 72, 74.

*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 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?*

Response to Questions 5 & 6:

As stated above, the purpose of the certification proposed in the NPRM is to ensure a clear set of rules and strong enforcement authority. The Federal Trade Commission, state attorneys general, and private litigants are generally able to pursue businesses that misrepresent their security and privacy practices. We anticipate that we and our partners at FTC would vigorously protect public interest features in competitive devices and apps, in much the same way that FCC already protects those same features in cable and satellite provider devices and apps. The NPRM seeks comment on these certification and enforcement mechanisms.

As further noted above, our record reflects filings from both the Federal Trade Commission and a group of state attorneys general—representing the states of California, Illinois, New York, Connecticut, Iowa, Maine, Maryland, Massachusetts, Minnesota, Mississippi, New Jersey, Oregon, Pennsylvania, Vermont, and the District of Columbia—stating that they would each be willing and able to enforce the privacy commitments made by third-party app and device manufacturers just as they currently enforce other privacy commitments made by apps and devices. I am confident that by working with stakeholders and our federal and state partners, we will identify clear rules of the road that will afford consumers with strong privacy protections and the enforcement mechanisms necessary to ensure compliance by third parties.

*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? 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?*

Response to Questions 7 & 8:

The FCC protects security and privacy in the current, noncompetitive set-top box ecosystem by requiring cable and satellite services to implement reasonable safeguards for customer

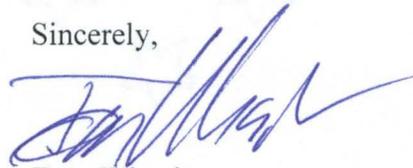
information.<sup>20</sup> The Commission protects telephone<sup>21</sup> and broadband<sup>22</sup> customer information by applying the same standard, and the Federal Trade Commission also evaluates security and privacy practices for their overall reasonableness.<sup>23</sup>

Whether a business's data safeguards are reasonable depends on the totality of the circumstances, including the sensitivity of the information, the nature of the business, and the risk of unauthorized access. How a business stores data, and where, are important components of the reasonableness standard.

Our proposal would apply the same reasonableness standard to competitive set-top boxes and apps. Should a competitive vendor fail to reasonably protect customer information, such as by storing it in unsafe circumstances, the FTC and state attorneys general could take corrective enforcement action? We would refer you to those agencies for questions about their investigative processes and regulatory remedies.

The record we are developing will help us preserve strong security and privacy protections while delivering American consumers meaningful choice. Thank you for your engagement in this proceeding, and I look forward to continuing to work with you on this important consumer issue.

Sincerely,



Tom Wheeler

---

<sup>20</sup> *E.g.*, Cox Communications, Inc. Order and Consent Decree, 30 FCC Rcd. 12302 (Nov. 5, 2015).

<sup>21</sup> *E.g.*, AT&T Services, Inc. Order and Consent Decree, 30 FCC Rcd. 2808 (Apr. 8, 2015).

<sup>22</sup> Open Internet Privacy Standard Enforcement Advisory, 30 FCC Rcd. 4849 (May 20, 2015).

<sup>23</sup> See FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 24-26 (2012).



FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

OFFICE OF  
THE CHAIRMAN

July 11, 2016

The Honorable Mike Pompeo  
U.S. House of Representatives  
436 Cannon House Office Building  
Washington, D.C. 20515

Dear Congressman Pompeo:

Thank you very much for sharing your questions about how the Commission's proceeding for better fostering competition in the set-top box and navigation app marketplace might impact security and privacy issues. I take your input on these issues seriously and assure you that it will receive careful consideration.

Protecting the nation's networks is a top priority for the FCC. Commission personnel work around the clock—including in a 24/7 operations center—to safeguard America's telephone, radio, cable, satellite, and Internet connectivity. The Commission takes our security responsibilities very seriously, and we leverage extensive staff expertise to ensure our policy proposals accord with best practices and the best available science.

We bring this cybersecurity experience and awareness to all of the rulemakings we undertake to fulfill our responsibilities under the Communications Act, including our current efforts to update our rules implementing section 629 of the Act. Section 629 of the Communications Act, adopted by Congress in 1996, requires the Commission to promote competition in the market for devices that consumers use to access their pay-television content. Yet, unfortunately, the statutory mandate in section 629 is not yet fulfilled. The lack of competition in this market has meant few choices and high prices for consumers. In a recent Rasmussen Report Study, 84 percent of consumers felt their cable bill was too high. One of the main contributing factors to these high prices is the no-option, add-on fee for set-top box rental that is included on every bill, forcing consumers to spend, on average, \$231 in rental fees annually. Even worse, a recent congressional investigation found that the price of most equipment fees is determined by what the market will bear, and not the actual cost of the equipment.<sup>1</sup> With the lack of competition in this market, it should come as little surprise that fees for set-top boxes continue to rise.<sup>2</sup> Clearly, consumers deserve better.

This February the Commission put out for public comment a proposal that would fulfill the statutory requirement of competitive choice for consumers. This action opened a fact-finding

---

<sup>1</sup> U.S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS COMMITTEE, MINORITY STAFF REPORT, *INSIDE THE BOX: CUSTOMER SERVICE AND BILLING PRACTICES IN THE CABLE AND SATELLITE INDUSTRY*, 17 (Jun. 23, 2016).

<sup>2</sup> One recent analysis found that the cost of cable set-top boxes has risen 185 percent since 1994 while the cost of computers, television and mobile phones has dropped by 90 percent during that same time period.

dialog to build a record upon which to base any final decisions. Our record already contains more than 280,000 filings, the overwhelming majority of which come from individual consumers. My staff is actively engaged in constructive conversations with all stakeholders—content creators, minority and independent programmers, public interest and consumer groups, device manufacturers and app developers, software security developers, and pay-TV providers of all sizes—on how to ensure that consumers have the competition and choice they deserve. I am hopeful that these discussions will yield straightforward, feasible, and effective rules for all.

You raise questions about how this proceeding might affect the network security protections currently in place. The Notice of Proposed Rulemaking (NPRM) adopted in February proposes a careful balance between network security and section 629's mandate that consumers be able to enjoy pay-television content with the equipment of their choice. Cable and satellite providers would be required to support a narrow, defined set of interfaces that would allow competitive devices and apps to access television content. These types of interfaces, usually termed Application Programming Interfaces (APIs), are routinely offered by online services. APIs allow a third party (such as a competitive navigation device provider) to interface with an organization's systems, without revealing any internal design, operation, or data about the organization. Third parties that connect to an API are not granted full system access, and are limited to only the features provided by the API. Securing an API is easier than securing internal systems, because an API only has to support specific functionality. Best practices for API security are readily available and widely practiced.<sup>3</sup>

The NPRM proposal would bring to television services the same secure modularity that phone and Internet customers have long enjoyed. In the telephone context, for example, a user can purchase and operate a third-party (e.g. Samsung) phone; the phone is not granted full access to telephone carrier (e.g. Verizon) internal systems. Similarly, in the Internet context, a user can purchase and operate a third-party (e.g. Arris) modem; that modem is not granted full access to the Internet Service Provider's (e.g. Comcast) internal systems.

All of the major cable and satellite providers, in fact, already support APIs for authenticating user credentials—some of the most sensitive information in the television ecosystem. Services like HBO Go<sup>4</sup> and Showtime Anytime<sup>5</sup> ensure that customers have subscribed by interfacing with cable and satellite account management systems. These APIs have been supported for over 5 years.

Further, the FCC's set-top box proposal will protect the role of digital rights management (DRM) platforms in the television ecosystem. DRM platforms offer rigorous protection against

---

<sup>3</sup> See, e.g., *OWASP Enterprise Security API Project*, OPEN WEB APPLICATION SOC'Y PROJECT [https://www.owasp.org/index.php/Project\\_Information:\\_OWASP\\_Enterprise\\_Security\\_API\\_Project](https://www.owasp.org/index.php/Project_Information:_OWASP_Enterprise_Security_API_Project) (last visited June 2, 2016).

<sup>4</sup> HBO GO, <http://play.hbogo.com> (last visited June 2, 2016).

<sup>5</sup> SHOWTIME ANYTIME, <http://www.showtimeanytime.com> (last visited June 2, 2016).

unauthorized copying and other violations of content owner rights.<sup>6</sup> Under the FCC's proposal, content owners would remain free to select the DRM platforms that they prefer. Developers of competitive set-top boxes and apps would license the DRM technology and satisfy compliance requirements – in the very same way that current set-top boxes support DRM, and the same way that competitive devices and apps already support DRM for online video. Furthermore, all of the major DRM platforms support revoking authorization for content; if a competitive device or app were ever found to be violating DRM requirements, access to content could be immediately terminated.

You also raise questions about how this proceeding might affect the privacy protections afforded to subscribers of pay-TV. As you know, pay-TV providers are obligated to comply with the privacy obligations imposed by Sections 631 and 338 of the Communications Act. These privacy obligations, among other things, prohibit pay-TV providers from disclosing personally identifiable information concerning any subscriber, including data about a subscriber's viewing habits, without the subscriber's prior consent.

I strongly believe that third-party app developers and device manufacturers must afford consumers the same level of protection as afforded by pay-TV providers. While the NPRM proposes that competitive devices and apps certify compliance with the privacy protections in the Act, we also invited parties to provide alternative proposals that would ensure the preservation of these important privacy protections.

We will continue to engage with stakeholders on this important issue. Notably, our record includes filings on this issue from the Federal Trade Commission (FTC) and a group of state attorneys general (state AGs)—representing the states of California, Illinois, New York, Connecticut, Iowa, Maine, Maryland, Massachusetts, Minnesota, Mississippi, New Jersey, Oregon, Pennsylvania, Vermont, and the District of Columbia. In their comments, the FTC and the state AGs explain that—if we require competitive devices and apps to publicly commit to providing the same privacy protections required of pay-TV providers under the Communications Act—the FTC and the state AGs would be willing and able to enforce the privacy commitments made by third-party app and device manufacturers just as they currently enforce other privacy commitments made by apps and devices. I am confident that by working with stakeholders and our federal and state partners, we will identify clear rules of the road that will afford consumers with strong privacy protections and the enforcement mechanisms necessary to ensure compliance by third parties.

Please find below answers to the specific questions in your letter.

*1a. Has the FCC considered the security implication 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.*

---

<sup>6</sup> See DOWNLOADABLE SEC. TECH. ADVISORY COMM., DSTAC FINAL REPORT 262-67 (Aug. 28, 2015), <https://transition.fcc.gov/dstac/dstac-report-final-08282015.pdf> [hereinafter DSTAC FINAL REPORT].

The NPRM was prompted in part by a congressional directive within the STELA Reauthorization Act of 2014.<sup>7</sup> Section 106(d) of that legislation required FCC to assemble a working group of technical experts to evaluate and recommend options for enhancing downloadable security systems designed to promote the competitive availability of navigation devices. The FCC promptly implemented Congress's directive by chartering the Downloadable Security Technology Advisory Committee (DSTAC) on December 5, 2014.

This DSTAC's membership consisted of diverse technical experts, drawn from content creators, cable and satellite providers, consumer electronics manufacturers, software vendors, public interest organizations, and academia.<sup>8</sup> The group first convened on February 23, 2015. After weekly conference calls and additional in-person meetings, the committee issued its final 344-page report on August 28, 2015.<sup>9</sup> The FCC also received over 100 comments and other submissions in association with this process.<sup>10</sup> You can find this report and other DSTAC materials at: <https://www.fcc.gov/about-fcc/advisory-committees/general/downloadable-security-technology-advisory-committee>.

The DSTAC's participants and commenters provided valuable technical guidance to the Commission, with particular emphasis on security and privacy matters. Over 100 pages of the committee's final report expressly address cable and satellite network security, protecting content, or safeguarding consumer data.<sup>11</sup> Many comments and submissions also addressed security issues.

In addition, as addressed above, the NPRM proposes to secure access to networks through the use of APIs. Third parties that connect to an API are not granted full system access, and are limited to only the features provided by the API. Securing an API is easier than securing internal systems, because an API only has to support specific functionality. In this way, the NPRM proposal would bring to television services the same secure modularity that phone and Internet customers have long enjoyed, without increasing malware risks for network operators.

Further, as also addressed above, the FCC's proposal will ensure that anti-piracy protections remain in place. Our proceeding will protect the role of DRM platforms in the television ecosystem. The NPRM proposed that content owners would remain free to select the DRM platforms that they prefer. Developers of competitive apps and set-top boxes would license the DRM technology and satisfy compliance requirements – in the very same way that current set-top boxes support DRM, and the same way that competitive apps and devices and already support DRM for online video.

---

<sup>7</sup> STELA Reauthorization Act of 2014, Pub. L. No. 113-200, § 106(d), 128 Stat. 2059 (2014)

<sup>8</sup> *Appointment of Members to the Downloadable Security Technology Advisory Committee*, 30 FCC Rcd 389 (Jan. 27, 2015).

<sup>9</sup> DSTAC FINAL REPORT, *supra* note 9.

<sup>10</sup> See MB Docket No. 15-64.

<sup>11</sup> See DSTAC FINAL REPORT, *supra* note 9, at 3-4, 12-16, 24-26, 28-30, 31-37, 47-56, 60-135, 186-192.

In sum, the FCC solicited and benefited from a wealth of security expertise while developing the proposed rulemaking, and we carefully evaluated the input that we received. The Notice of Proposed Rulemaking seeks additional input from stakeholders on the security aspects of the Commission's proposal.<sup>12</sup> The Commission will not take any actions that would increase network vulnerabilities or reduce anti-piracy protections.

*1b. Has the FCC assessed the potential economic impact of 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.*

In light of our comprehensive approach to security issues, our proposal does not increase the risk of identity theft to consumers or the risk of economic harm as a result of security breaches to copyright owners/creators or businesses. As addressed herein and consistent with our duty under section 629(b) to protect system security and sections 631 and 338 to protect subscriber privacy, our proposal protects the integrity of television delivery systems and the rights of content owners. Consumers will have the very same legal remedies available to them today to pursue individuals engaged in identify theft, and content creators will have the very same legal remedies available to them today to pursue individuals who pirate content<sup>13</sup> or circumvent copy protections.<sup>14</sup> Similarly, our proposal would not affect the legal remedies available to U.S. businesses to pursue hackers.<sup>15</sup>

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

*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?*

The Communications Act and Commission rules guarantee a set of public interest protections for current cable and satellite set-top subscribers.<sup>16</sup> These features include strong security and privacy protections, Emergency Alert System messaging, closed captioning, parental controls, and limits on advertising to children. If a cable or satellite provider fails to satisfy these requirements, the Commission is able to ensure corrective measures by initiating an enforcement action.<sup>17</sup>

---

<sup>12</sup> Expanding Consumers' Video Navigation Choices, Notice of Proposed Rulemaking, 31 FCC Rcd 1544, 1568-74, 1576-83, ¶¶ 50-62, 70-80.

<sup>13</sup> E.g., 47 U.S.C. §§ 501-506 (civil cause of action and criminal penalties for copyright infringement).

<sup>14</sup> E.g., 17 U.S.C. § 1201 (civil cause of action and criminal penalties for circumventing content protections).

<sup>15</sup> E.g., 18 U.S.C. § 1030 (civil cause of action and criminal penalties for computer trespass).

<sup>16</sup> Expanding Consumers' Video Navigation Choices, *supra* note 12, 1579-80, ¶ 73.

<sup>17</sup> E.g., Cox Communications, Inc. Order and Consent Decree, 30 FCC Rcd. 12302 (Nov. 5, 2015) (enforcement action against a cable provider that did not adequately secure customer information).

The NPRM seeks to ensure that these important and longstanding public interest features continue to be guaranteed in competitive set-top boxes and video apps that access cable and satellite content. We propose accomplishing this goal through a certification process, in which third-party devices' and apps' interoperability with cable and satellite networks will be conditioned on the devices' and apps' compliance with these public interest features.

The Federal Trade Commission, state attorneys general, and private litigants are generally able to pursue businesses that misrepresent their security and privacy practices. We anticipate that we and our partners at FTC would vigorously protect public interest features in competitive devices and apps, in much the same way that FCC already protects those same features in cable and satellite devices and apps. The NPRM seeks comment on these certification and enforcement mechanisms.

*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?*

Response to Questions 3 & 4:

A business that offers a competitive set-top box or video app that accesses cable and satellite content would commit to adopting reasonable security safeguards and privacy safeguards consistent with Sections 338 and 631 of the Act. The purpose of this certification is to ensure a clear set of rules and strong enforcement authority. The NPRM seeks comment on the best certification process, whether certification to consumers, certification to cable and satellite providers, certification to the Commission, or certification to an independent body to ensure compliance. If a device manufacturer or software vendor failed to implement adequate precautions, it would risk enforcement action under the Federal Trade Commission Act and similar state statutes. Cable and satellite providers could also revoke interoperability with that set-top box or video app.

Under the proposal set forth in the NPRM, a competitive device or app could also be subject to technical auditing for ensuring adequate content protection. The NPRM's proposal would not alter the current landscape of DRM platforms, some of which require technical validation for a device or app to be compliant.<sup>18</sup> The NPRM seeks comment on whether independent testing should be required for other navigation device security properties.<sup>19</sup>

*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*

---

<sup>18</sup> Expanding Consumers' Video Navigation Choices, *supra* note 1, ¶ 71.

<sup>19</sup> *Id.* ¶¶ 72, 74.

*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 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?*

Response to Questions 5 & 6:

As stated above, the purpose of the certification proposed in the NPRM is to ensure a clear set of rules and strong enforcement authority. The Federal Trade Commission, state attorneys general, and private litigants are generally able to pursue businesses that misrepresent their security and privacy practices. We anticipate that we and our partners at FTC would vigorously protect public interest features in competitive devices and apps, in much the same way that FCC already protects those same features in cable and satellite provider devices and apps. The NPRM seeks comment on these certification and enforcement mechanisms.

As further noted above, our record reflects filings from both the Federal Trade Commission and a group of state attorneys general—representing the states of California, Illinois, New York, Connecticut, Iowa, Maine, Maryland, Massachusetts, Minnesota, Mississippi, New Jersey, Oregon, Pennsylvania, Vermont, and the District of Columbia—stating that they would each be willing and able to enforce the privacy commitments made by third-party app and device manufacturers just as they currently enforce other privacy commitments made by apps and devices. I am confident that by working with stakeholders and our federal and state partners, we will identify clear rules of the road that will afford consumers with strong privacy protections and the enforcement mechanisms necessary to ensure compliance by third parties.

*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? 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?*

Response to Questions 7 & 8:

The FCC protects security and privacy in the current, noncompetitive set-top box ecosystem by requiring cable and satellite services to implement reasonable safeguards for customer

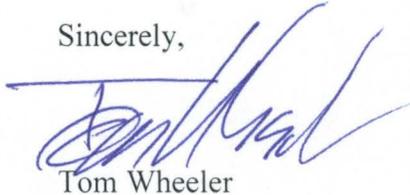
information.<sup>20</sup> The Commission protects telephone<sup>21</sup> and broadband<sup>22</sup> customer information by applying the same standard, and the Federal Trade Commission also evaluates security and privacy practices for their overall reasonableness.<sup>23</sup>

Whether a business's data safeguards are reasonable depends on the totality of the circumstances, including the sensitivity of the information, the nature of the business, and the risk of unauthorized access. How a business stores data, and where, are important components of the reasonableness standard.

Our proposal would apply the same reasonableness standard to competitive set-top boxes and apps. Should a competitive vendor fail to reasonably protect customer information, such as by storing it in unsafe circumstances, the FTC and state attorneys general could take corrective enforcement action? We would refer you to those agencies for questions about their investigative processes and regulatory remedies.

The record we are developing will help us preserve strong security and privacy protections while delivering American consumers meaningful choice. Thank you for your engagement in this proceeding, and I look forward to continuing to work with you on this important consumer issue.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Tom Wheeler', is written over a horizontal line.

Tom Wheeler

---

<sup>20</sup> *E.g.*, Cox Communications, Inc. Order and Consent Decree, 30 FCC Rcd. 12302 (Nov. 5, 2015).

<sup>21</sup> *E.g.*, AT&T Services, Inc. Order and Consent Decree, 30 FCC Rcd. 2808 (Apr. 8, 2015).

<sup>22</sup> Open Internet Privacy Standard Enforcement Advisory, 30 FCC Rcd. 4849 (May 20, 2015).

<sup>23</sup> See FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 24-26 (2012).