

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554**

*In the Matter of*

**Protecting the Privacy of Customers of  
Broadband and Other Telecommunications  
Services**

WC Docket No. 16-106

**COMMENTS OF HUGHES NETWORK SYSTEMS, LLC**

Hughes Network Systems, LLC (“Hughes”) submits these comments in response to the Commission’s Notice of Proposed Rulemaking (the “*Notice*”),<sup>1</sup> which proposes rules governing the privacy of customer proprietary information (“customer PI”)<sup>2</sup> that would apply to all providers of broadband Internet access service. Many of the Commission’s proposals, including requiring clear notice of privacy policies, obtaining and tracking consent, and maintaining data security, reflect widespread industry practices and are consistent with Hughes’, the largest U.S. satellite broadband service provider, existing sound privacy practices.

However, based on our experience in the marketplace, Hughes provides proposed refinements to several of the FCC’s proposals. Specifically, Hughes proposes that:

- The FCC provide broadband service providers with voluntary safe harbors for disclosing broadband privacy policies, and consumers with flexible mechanisms for providing and updating their privacy preferences;
- The FCC set clear deadlines for broadband service providers to act on consumer consent modifications and to notify affected consumers, the Commission and other appropriate agencies of significant data breaches;

---

<sup>1</sup> See *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (2016) (“*Notice*”).

<sup>2</sup> As proposed by the Commission, customer PI would include both customer proprietary network information (CPNI) and personally identifiable information (PII). *Id.* at ¶ 15.

- Any adopted broadband privacy rules should preempt inconsistent state laws;
- The FCC should preserve the ability of consumers to agree to arbitration; and
- The FCC should shorten the proposed time of the recordkeeping requirement.

## **BACKGROUND**

Hughes is the global leader in satellite broadband solutions and services and a leading provider of managed network services and applications. In the United States, HughesNet is the largest satellite broadband service provider, serving over one million subscribers today with speeds of up to 15 Mbps, which will increase to approximately 25 Mbps after the launch of the high-throughput Jupiter 2 satellite later this year.

As a broadband service provider entrusted with safeguarding consumer privacy, Hughes has already made a commitment through its customer privacy policy to ensuring the integrity of customer PI. Protecting consumer data is part of Hughes' broader commitment to providing transparency and clear disclosures to its subscribers.<sup>3</sup> Hughes agrees with the FCC that all broadband service providers should maintain—and enforce—rigorous data privacy policies. Hughes looks forward to working with the Commission to ensure the broad adoption of data privacy best practices by all broadband service providers, including satellite broadband providers.

## **DISCUSSION**

### **I. CLEAR PRIVACY NOTICES AND VOLUNTARY SAFE HARBORS WILL ENHANCE CONSUMER PRIVACY**

---

<sup>3</sup> For example, in 2015 the FCC found in its Measuring Broadband America report that our Gen4 satellite broadband service ranked first among all major Internet service providers for delivering on advertised performance promises. See FCC, *Measuring Broadband America* (rel. Dec. 30, 2015), <https://www.fcc.gov/reports-research/reports/measuring-broadband-america/measuring-broadband-america-2015>.

Hughes values the privacy of each of its customers. Accordingly, Hughes supports the FCC's goal in protecting customer PI by adopting privacy policies that empower consumers with greater control over their important personal information. Hughes' privacy policies reflect that commitment today as Hughes provides all consumers with 24 hour access to our plain language privacy policy on our website.<sup>4</sup> Accordingly, Hughes, an early adopter of consumer privacy protections, fully supports the FCC requiring all broadband providers to provide clear, transparent privacy disclosures on their website to prospective customers and current subscribers.<sup>5</sup>

However, Hughes has concerns about the FCC's proposal that broadband service providers be required to supply "layered" privacy notices.<sup>6</sup> Not only is such a requirement unnecessary, but it would likely result in customer confusion because consumers would have to read through and understand several layers of disclosures. A better approach is for the FCC to require broadband providers to provide a minimum level of information to customers. With such a baseline, broadband service providers would be able to best develop a format that is clear and gives customers the information they require.

Accordingly, Hughes supports the Commission's proposal to allow broadband service providers to voluntarily use a "nutrition label" template for online privacy policy disclosure notices that would serve as a safe harbor.<sup>7</sup> Making available a safe harbor format for privacy policies would benefit consumers by increasing the homogeneity of such disclosures and enhancing consumers' ability to compare key aspects of providers' privacy policies on their websites. The proposed voluntary safe harbor approach would also be beneficial for broadband

---

<sup>4</sup> See Hughes Subscriber Privacy Policy, <http://legal.hughesnet.com/SubscriberPolicies.cfm>.

<sup>5</sup> Notice at ¶ 87.

<sup>6</sup> *Id.* at ¶ 94.

<sup>7</sup> *Id.* at ¶¶ 90-92.

service providers by reducing their compliance burden and increasing the certainty that policy disclosures comply with FCC requirements. However, Hughes urges the FCC to make the use of this nutrition label voluntary.<sup>8</sup> As long as broadband service providers are in compliance with FCC disclosure requirements, they should have the option to tailor their privacy disclosures to the needs of their subscribers.<sup>9</sup>

## **II. CONSUMERS SHOULD HAVE MAXIMUM FLEXIBILITY IN PROVIDING AND UPDATING CONSENT**

The *Notice* proposes a consent hierarchy designed to enhance the ability of consumers to make informed decisions about how, and by whom, their customer PI can be used.<sup>10</sup> The consent hierarchy proposed by the Commission reflects a common sense approach to treating customer PI according to consumer expectations.<sup>11</sup>

As proposed, consumers would be able to opt-in or opt-out of consent at the time they subscribe to a service, and update their consent selections with their provider at any time. The Commission seeks comment on whether carriers should be required to “refresh” opt-in or opt-out consent periodically.<sup>12</sup> This is not necessary. The optimal solution would be to ensure that broadband service providers inform consumers of their privacy options and update consumers’ decisions regarding privacy preferences when they are affirmatively communicated to their

---

<sup>8</sup> Should the Commission require mandatory use of the nutrition label, use of this format should be limited to website disclosures which can quickly be updated and should not extend to printed consumer-directed materials that would be costly and burdensome to revise with service changes.

<sup>9</sup> In the context of data security, the Commission asks whether it should adopt safe harbors or alternatively convene stakeholders to establish best practices. *Id.* at ¶ 178. Hughes recommends that the Commission draw from its own expertise to incorporate safe harbors into its final rules, rather than delegating the development of best practices to a federal advisory committee, which could delay the issuance of guidance for broadband service providers.

<sup>10</sup> *Id.* at ¶ 106.

<sup>11</sup> Hughes supports the Commission’s proposal to find that certain types of customer PI are sufficiently “highly sensitive” that consumers should be required to opt-in for its use by broadband service providers. *Id.* at ¶ 136. A heightened designation for information such as social security numbers, financial information, geo-location information, and information on children or consumer health would protect consumers and would not impede the ability of broadband service providers to ensure quality service to their subscribers.

<sup>12</sup> *Id.* at ¶ 257.

service provider. Requiring broadband providers to periodically require customers to refresh their privacy choices might be counterproductive and lead to increased consumer confusion. A better approach would be to allow broadband service providers to have a link on the same webpage as their privacy policy, which customers can click on to review and, if warranted, change their privacy preferences. This voluntary compliance mechanism would provide consumers with immediate access and control over their privacy preferences and would make it easier for broadband service providers to ensure that they are treating customer PI in accordance with consumers' preferences.

The Commission also proposes that broadband service providers be required to make available a dashboard or other online user interface that consumers could use to view existing privacy preferences and deny or grant approval for use of their customer PI by their provider.<sup>13</sup> While a dashboard approach may make sense for some broadband service providers, if the broadband service provider otherwise meets the FCC's privacy requirements, there is no need for the FCC to make a dashboard mandatory. Broadband subscribers should be able to confirm or amend their privacy settings through the mechanism—communicated as part of the privacy policy provided to all subscribers—with which they are most comfortable, which may not be an online dashboard. While some consumers would be willing to use a dashboard interface, many consumers are more comfortable communicating directly with their service provider via phone, chat, e-mail or postal mail.<sup>14</sup> If the Commission does require providers to use a dashboard to

---

<sup>13</sup> *Id.* at ¶¶ 144-45.

<sup>14</sup> Studies suggest that live chat features and e-mail are American consumer's preferred method of interacting with customer service representatives. *See, e.g.*, "Which Customer Service Channels Do Consumers Prefer," Smart Insights (Mar. 4, 2015), <http://www.smartinsights.com/customer-relationship-management/customer-service-and-support/customerservicechannels/>; "52% of Consumers Prefer Text Conversations with Support Reps over their Current Support Method," Business Wire (Apr. 4, 2014), <http://www.businesswire.com/news/home/20140402005509/en/52-Percent-Consumers-Prefer-Text-Conversations-Support>.

accept consumer privacy preference inputs and updates, just as with the proposed nutrition label it should provide a template that would serve as a safe harbor for broadband service providers.

Consumers deserve quick action when amending their privacy preferences. The *Notice* proposes that broadband service providers be required to act “promptly” upon customers’ privacy choices after subscribers provide or withdraw consent for the use or disclosure of their information, but does not define “promptly.”<sup>15</sup> Adopting a timeline for addressing consumers’ privacy decisions would allow consumers certainty regarding when their revised preferences will be put into effect and ensure that providers do not delay in honoring such requests. The Commission should allow broadband service providers 10 business days to implement a consumer’s request to opt-in or opt-out of permitted uses of their customer PI. A 10 business day window would allow a provider sufficient time to process and, if necessary, confirm the consumers’ request, update all internal databases, and communicate the revised consent with affiliated and outside parties.

### **III. DATA SECURITY REQUIREMENTS SHOULD BE STRAIGHTFORWARD AND NOT REDUNDANT**

The *Notice* proposes that no later than 10 days following discovery of a breach of data privacy a broadband service provider should notify customers affected by that breach.<sup>16</sup> However, the Commission’s proposal could leave broadband service providers with inadequate time to adequately assess a reported data breach. Although broadband service providers remain vigilant around the clock to detect, diagnose and shut down potential data breaches, attacks mounted by cyber criminals today are increasingly sophisticated and require significant resources to analyze and assess. Rather than requiring broadband service providers to complete their analysis of a breach and compile required reports within the relatively short period of 10

---

<sup>15</sup> *Id.* at ¶ 147.

<sup>16</sup> *Id.* at ¶¶ 236-242.

calendar days, a more equitable solution would be to stipulate that broadband service providers must report a breach within 30 days from the discovery of that breach, with leave to extend the reporting period by 30 day increments if the broadband service provider can demonstrate that more time is needed to determine the scope of the breach, to conduct risk assessments, and to restore reasonable integrity to the network.<sup>17</sup> This minimal modification of the proposed rule will give time for quick action while recognizing the real time needed accurately to respond to a reported breach. To ease compliance and avoid confusion, the same 30 day renewable time frame should also apply to notices to the Commission and relevant law enforcement agencies, rather than seven days as currently proposed.<sup>18</sup>

Hughes also supports the FCC preempting state privacy laws to the extent that they are inconsistent with any rules adopted by the Commission.<sup>19</sup> Failure to preempt such laws would result in broadband service providers diverting valuable resources from notifying affected customers and remedying the breach. Further, it is important that the FCC preempt these laws in total on the effective date of these rules, and not on a case by case basis. Failure to do so will add unnecessary administrative burdens on broadband service providers, and more importantly, divert valuable resources away from resolving privacy issues that arise.

Finally, the Commission should adopt the *Notice*'s proposal that each broadband service provider be able to determine the particulars and design of its own risk management program to

---

<sup>17</sup> Providing renewable 30 day periods in which to provide notice would align the Commission's proposal with the Personal Data Notification and Protection Act of 2015 ("Act"), which proposes a national 30 day standard for data breach notification. *See* H.R. 1704. The Act also provides a safe harbor for covered business entities that have conducted a risk assessment and found that there is no reasonable risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach and that notify the Federal Trade Commission of the results of this assessment within 30 days. The Commission should considering adopting this reasonable proposed safe harbor as part of any broadband privacy rules.

<sup>18</sup> *Notice* at ¶ 239.

<sup>19</sup> *Id.* at ¶ 276.

identify and protect against risks to the security, confidentiality, and integrity of customer PI.<sup>20</sup> The Commission does not need to require periodic technical audits such as penetration tests<sup>21</sup> because broadband providers that accept payment by credit card are already subject to such testing as part of the Payment Card Industry Data Security Standard (PCI DSS).<sup>22</sup>

#### IV. CONSUMERS SHOULD BE FREE TO ENTER INTO ARBITRATION AGREEMENTS

In the *Notice* the Commission acknowledges the utility of arbitration in resolving consumer privacy disputes.<sup>23</sup> As the Commission is aware, arbitration is frequently used by broadband service providers to expedite resolution of disputes and reduce costs incurred in litigation, allowing savings to be passed directly to consumers.<sup>24</sup> In the 2015 *Open Internet Order*, the Commission considered—and rejected—proposals that would interfere with the ability of broadband service providers and consumers to agree to resolve disputes through arbitration.<sup>25</sup> Similarly here, the Commission should permit broadband service providers to continue to include arbitration clauses in customer privacy agreements. Like all other aspects of

---

<sup>20</sup> *Id.* at ¶¶ 180-184.

<sup>21</sup> *Id.* at ¶ 181.

<sup>22</sup> Because of the important privacy issues at stake, PCI continuously updates and revises its standards to ensure that vendors that accept credit cards adopt state-of-the-art physical and logical security and resilient internal processes. See Payment Card Industry Security Standards Council, Maintaining Payment Security, [https://www.pcisecuritystandards.org/pci\\_security/maintaining\\_payment\\_security](https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security). In addition to required PCI DSS annual penetration tests, Hughes continuously conducts vulnerability scans and maintains best practice protection, including state of the art firewalls and advanced malware detection systems of all of our systems, throughout the enterprise. Our internal security teams also collaborate with our internal audit group to ensure that we are in compliance with our own risk management and security program.

<sup>23</sup> *Notice* at ¶ 274.

<sup>24</sup> The Supreme Court has recently affirmed that the Federal Arbitration Act (FAA) operates broadly to support the validity of agreed-upon arbitration clauses. *AT&T Mobility v. Concepcion*, 563 U.S. 333 (2011); see also FAA, 9 U.S.C. § 2. Studies have found that arbitration can increase recovery rates for consumers and enable consumers to avoid high attorney's fees inherent in most class action lawsuits, and the average customer who prevailed in arbitration received 166 times more in financial payments than the average class member in class action settlements. See Letter from American Bankers Association *et al.* to Richard Cordray, Director, Consumer Financial Protection Bureau (CFPB) (July 13, 2015), <https://www.cfpbmonitor.com/wp-content/uploads/sites/5/2015/07/March-10-2015-Consumer-Arbitration-Study-Comment-Letter.pdf>; Jason Scott Johnston & Todd Zywicki, *A Summary and Critical of the CFPB's Arbitration Study* (Aug. 2015), <http://mercatus.org/sites/default/files/Johnston-CFPB-Arbitration.pdf>.

<sup>25</sup> *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 at ¶ 267 (2015).

a service provider's privacy policy, reasonable arbitration clauses should be clear and transparent. Ultimately, both consumers and service providers would benefit from the continued availability of dispute resolution mechanisms that allow complaints to be resolved by professional arbitrators outside of the courtroom.

#### **V. LIMITING RECORDKEEPING REQUIREMENTS WILL EXPEDITE INFORMATION RETRIEVALS AND AVOID LEGAL RISK**

Hughes understands the importance of requiring broadband service providers to retain customer records, which will assist law enforcement entities in their investigations and allow the Commission and providers to respond to consumer inquiries. However, any retention policy must balance the benefits of the length of retention and the administrative burdens such a requirement imposes. It would be reasonable to require broadband service providers to retain a record of any discovered breaches and notifications to the FBI, the Secret Service, and customers for six months, rather than two years as the Commission initially proposed.<sup>26</sup> A six month recordkeeping requirement will ensure that customers' records are retained for a reasonable period following the termination of service and give the Commission and law enforcement agencies sufficient access to records to conduct investigations of consumer complaints. Moreover, there is no need to extend data retention for two years because in Hughes' experience, no information request or subpoena from a law enforcement agency has sought breach data going back farther than six months. By contrast, retaining customer records for longer than six months, rather than destroying outdated information, would heighten legal risk by increasing the amount of customer PI that could potentially be subject to a data breach and would impose unnecessary administrative burdens and data storage and processing costs on broadband service providers.<sup>27</sup>

---

<sup>26</sup> Notice at ¶¶ 252-53.

<sup>27</sup> See, e.g., *A Bill to Require Greater Protection of Sensitive Consumer Data and Timely Notification in Case of Breach*: Hearing on H.R. \_\_\_\_ Before the Subcomm. on Commerce, Manufacturing & Trade, H. Comm. on Energy &

## VI. CONCLUSION

In this proceeding the FCC has an opportunity to create a regulatory framework that will increase consumer confidence in the privacy of sensitive and personal information in the context of broadband service. By providing voluntary safe harbors that broadband service providers can use to disclose privacy policies; encouraging flexible mechanisms by which consumers can provide and update their privacy preferences; adopting straightforward data breach disclosure requirements; preserving the ability of consumers to agree to arbitration; and shortening the proposed recordkeeping requirement, the FCC can achieve this important goal.

Respectfully submitted,

*/s/ Jennifer A. Manner*

---

Jennifer A. Manner  
Senior Vice President, Regulatory Affairs  
Deborah Broderson  
Communications Regulatory Counsel and  
Director

HUGHES NETWORK SYSTEMS, LLC  
11717 Exploration Lane  
Germantown, MD 20876  
(301) 428-5893

May 27, 2016

---

*Commerce*, 112<sup>th</sup> Cong. 3 (2011) (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center) (citing risks of retaining data for unnecessarily long periods).