

**Before the  
Federal Communications Commission  
Washington, DC 20554**

In the Matter of )  
 )  
Protecting the Privacy of Customers of ) WC Docket No. 16-106  
Broadband and Other Telecommunications )  
Services )  
 )  
 )  
 )  
 )

---

**COMMENTS OF THE STATE PRIVACY AND SECURITY COALITION**

---

Jim Halpert  
Anne Kierig  
500 8th Street, NW  
Washington, D.C. 20004  
(202) 799-4441

May 27, 2016

## EXECUTIVE SUMMARY

The State Privacy and Security Coalition, Inc., a coalition of 25 leading communications, technology, retail, and media companies and six trade associations, respectfully submits these comments in response to the NPRM in the matter of “Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.”

The members of our coalition agree that the definitions, the strict liability information security and breach notice requirements of the NPRM’s proposal apply too broadly, and unless scaled back in the final rule, would have several serious unintended consequences for consumers, for information security practices, and for cybersecurity.

The current CPNI security rules differ markedly from state breach notice laws and both the final rule and the current security rules should be aligned with the well-established state approaches. Specifically, the NPRM proposal is broader than existing information security and breach notice requirements in that it would apply to a large range of information that is not sensitive, including even data that is publicly available or that travels widely around the Internet when users communicate. The NPRM proposal would require audit trails, access controls, and security breach notice for information that is not sensitive. It also would require notice in the absence of any harm trigger, with an unreasonably short breach notice deadline, and would fail to exempt good faith employee access to data that exceeds authorized access, among other things.

For these reasons, and the reasons articulated in these comments, we urge the Commission to make significant changes to the definitions of CPNI and customer proprietary information, to the audit log and access control requirements, and to the breach notice requirement in any final rule.

## TABLE OF CONTENTS

	<b>Page</b>
Executive Summary .....	2
I. INTRODUCTION .....	4
II. THE STATUTORY BASIS FOR THE BREADTH OF THE PROPOSED DATA SECURITY AND BREACH NOTICE REQUIREMENTS ARE HIGHLY QUESTIONABLE .....	5
III. THE NPRM PROPOSAL IS BROADER THAN INFORMATION SECURITY AND BREACH NOTICE REQUIREMENTS IN SIX SIGNIFICANT RESPECTS. ....	8
IV. CONCLUSION.....	17

## I. INTRODUCTION

The State Privacy and Security Coalition, Inc., a coalition of 25 leading communications, technology, retail, and media companies and six trade associations, respectfully submits these comments in response to the Notice of Proposed Rulemaking in the matter of “Protecting the Privacy of Customers of Broadband and Other Telecommunications Services” (the “Proposed Rules” or “NPRM”).

All of our members are concerned that the Commission’s proposed definitions and data security and breach notice requirements would create several unintended and unnecessary consequences that would do more harm than good for consumers. They would:

- (1) far exceed the requirements set forth in any current federal or state data security or information security law and conflict with accepted cybersecurity best practices and methods regarding risk prioritization;
- (2) impose significant and unnecessary costs not only on ISPs and their affiliates who store broadband customer data, but also on the larger ecosystem of service providers who may store or access it, potentially increasing the cost of providing services; and
- (3) create a very strong incentive for operators of critical infrastructure to implement extensive measures to secure, and to notify very quickly of access to, information that if breached would pose no risk whatsoever to consumers, including information that has been de-identified or that is widely available from other sources.

For consumers, the overbreadth in the NPRM’s proposed data security and breach notice requirements would be a net minus. These requirements would produce significant over-notification of consumers for breaches that pose no risk to them. The NPRM itself recognizes

“the harms inherent in over-notification.”<sup>1</sup> As to consumers, requiring notification in many situations that involve no risk of harm makes “notice fatigue” more likely with consumers ignoring notice of serious breaches that actually create risk. In addition, requiring several heavy security measures and rapid breach notice for information that is not sensitive would risk diverting ISP resources from preventing and remediating much more serious threats to ISP networks and their users.

We urge the Commission to revise the proposed definitions of customer proprietary network information (“CPNI”) and the very large new category of customer proprietary information to focus only on *sensitive* information, and to reserve the strong security obligations and unprecedented breach notice requirements for that sensitive information. We further urge the Commission to align its proposed breach notice requirements so that they do not exceed the longstanding requirements under state breach notice laws. Finally, we urge the Commission to revise its definition of de-identified data to make it fully consistent with the Federal Trade Commission’s (“FTC’s”) definition, as applied, and remove the proposed requirement that data be *both* de-identified *and aggregated*. These changes would create an FCC risk-based information security and breach notice regime that strongly protects consumers consistent with sound data and cybersecurity practices, and with privacy good practices.

---

<sup>1</sup> *In re* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Notice of Proposed Rulemaking*, FCC 16-39, WC Docket No. 16-106, ¶ 236 (March 31, 2016) (“NPRM”).

## II. THE STATUTORY BASIS FOR THE BREADTH OF THE PROPOSED DATA SECURITY AND BREACH NOTICE REQUIREMENTS IS HIGHLY QUESTIONABLE

The current CPNI security and breach notification rules<sup>2</sup> are an anomaly vis-à-vis security and breach notice laws and require significant changes if they are to work as to the Internet.

The CPNI statute was tailored specifically to telecomm competition as of 1996. It does not regulate more sensitive communications-related information, such as actual communications content, which is addressed in the Electronic Communications Privacy Act. Instead, it regulates information relating “to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier” and certain “information contained in” telephone bills pertaining to that service.<sup>3</sup> Information about technical configuration or type of service (for example, that a subscriber has an unlimited calling plan or receives 5 megabit per second broadband service) is not sensitive data. The information was highly relevant, though, in the late 1990s to a local exchange carrier that might try to capture a customer’s long distance business. The current CPNI statute exempts “subscribers’ telephone numbers, addresses, or primary advertising classifications” that a carrier or affiliate has published in a directory.<sup>4</sup> Unlike other privacy laws, it actually *requires* disclosure of subscriber list information to other carriers when a customer opts to switch to a competitor.<sup>5</sup>

---

<sup>2</sup> 47 C.F.R. § 64.2001, *et seq.*

<sup>3</sup> 47 U.S.C. § 222(h)(1).

<sup>4</sup> *Id.* § 222(h)(3).

<sup>5</sup> *Id.* § 222(d)(2).

The current rules that overlaid data security and breach notice requirements on this tranche of data were adopted in 2007 in response to national concern over “pretext calling” (mostly by private investigators) to obtain customer call detail records and by the sale of phone number records by Internet data brokers. The Commission structured its rules so that they apply only to CPNI, and made no mention of any of the much broader new category of customer proprietary information proposed in the NPRM. However, it lumped in *all* CPNI under these new requirements, including information about the type of service plans used by consumers, and details about their home phone equipment. It did this even though call detail records were the topic of specific legislative concern, according to the Committee reports regarding a bill that advanced in the House on the issue<sup>6</sup> but failed to pass in the Senate.

As there is no record of similar pretext calling or sale of broadband ISP Internet usage information, it is far from a foregone public policy conclusion that any of these data security or breach notice requirements should extend to Internet data, much less to the vast categories of non-sensitive information swept in by the NPRM’s proposed definitions.

Furthermore, the statutory basis for reaching a broad category of Internet data is shaky. The statutory language of Section 222(h)(1) is highly specific in referencing solely information that relates to “telephone service.”

The NPRM’s proposed rule would build over and expand very significantly on the existing CPNI structure, by creating a very broad new definition of “customer proprietary information” that includes a large amount of data that is not sensitive, by reading the statutory exception for “subscriber list information” out of the statute, and by adding several new security and privacy requirements.

---

<sup>6</sup> H. Rep. No. 109-398, at 2-3 (109th Cong. 2d Sess.)

While the Commission’s proposed rules may be well-intentioned, we believe strongly that they need to be pared back to make sense in the context of broadband Internet access service and to avoid misallocation of security resources and significant over-notification.

### **III. THE NPRM PROPOSAL IS BROADER THAN INFORMATION SECURITY AND BREACH NOTICE REQUIREMENTS IN SIX SIGNIFICANT RESPECTS**

In several places, the NPRM specifically references “state laws on breach notification, which inform our proposals” and acknowledges the harms inherent in over-notification (or ‘notice fatigue’).<sup>7</sup> However, the actual content of the Commission’s proposed breach notice rules differ markedly from the large body of state breach notice laws. The proposed rules would: (1) significantly expand the types of covered information beyond existing state information security and breach notice laws, including information that is not in the least sensitive and, in some cases, is broadly available, (2) use an “access” instead of an “acquisition” standard, (3) not include a risk of harm trigger that could limit customer over-notification, (4) not include a good faith employee acquisition or access exception, (5) impose unrealistic notification deadlines that cannot be met in most instances and could result in incomplete and/or inaccurate breach notices, and (6) jettison the “intentionality requirement” found in the CPNI rule’s current definition of a “breach.”

These differences really matter for several reasons. First, they would mandate over-notification in situations that pose no risk or materiality to consumers, increasing the risk that consumers will ignore notices of security events. Second, breach notice incidents are expensive. The average cost per record of a data breach including both out of pocket costs and harm to good will currently exceeds \$200 per record.<sup>8</sup> The Proposed Rules would, without justification,

---

<sup>7</sup> NPRM ¶¶ 23, 75, 236.

<sup>8</sup> Ponemon Institute. (2015). *2015 Cost of Data Breach Study: Global Analysis*.

increase significantly the number of breach notices that businesses will be required to send to consumers. This is not only wasteful; it also creates a strong incentive for businesses to prioritize protection of any information covered by a breach notice requirement over other information and network assets.

The proposed rule likewise effectively requires implementing audit logging in order to account for each event of access to or disclosure of the broad categories of CPNI and customer proprietary information to third parties. It also requires strong authentication measures to control access to all these data.<sup>9</sup>

Broadband ISPs would be required to institute heavy security measures and incentivized to start treating information that is not sensitive as a “crown jewel” that security attention and resources must be shifted to. At the very least, requiring breach notice for non-sensitive information, such as IP addresses or MAC addresses, is a security distraction. At worst, because security resources are usually finite, it would actually take resources away from the far more important task of protecting the resilience of broadband ISP critical infrastructure networks and network components.

For all these reasons, the Commission should reconcile the NPRM’s definition of what information must be protected and triggers a breach notification obligation, the range of its security requirements and its breach notice requirements with the well-established and effective state breach notice laws.

**A. Requiring Audit Trails, Security Measures and Breach Notice for Information That Is Not Sensitive**

The 47 state data security and data breach notice laws apply to the name of a state resident plus a sensitive data element. The sensitive data elements vary by state, but include

---

<sup>9</sup> NPRM, Exh. A, §§ 64.7003(b) & 64.7005(a)(4).

social security number, government identification number, financial account number in combination with a code to access a financial account, and in some states medical information, health insurance claim information or user name and password for an online account.<sup>10</sup> States have considered and uniformly rejected proposals to require notification of all personally identifiable information,<sup>11</sup> of websites visited by state residents,<sup>12</sup> and long lists of data elements,<sup>13</sup> all of which would be swept into the NPRM’s customer proprietary information definition and require notification in the case of a breach.

The NPRM *categorically* treats all CPNI and customer proprietary information as sensitive data and subjects it to audit trail and access control requirements and (impractically short) breach notice requirements. It starts from the assumption that *non-content* broadband Internet access provider data should all fit into the existing CPNI framework. This includes information such as IP addresses, MAC addresses, and browser type, that is disclosed across the Internet wherever users surf the web or communicate through other networks, and is in no way private. Indeed, this information is the equivalent in the Internet context of an element of “subscriber list information” which is exempt from the scope of the CPNI statute<sup>14</sup> and thus should be exempt from any final rule adopted by the Commission.

Notification is required if “any information that is linked or linkable to an individual” is accessed without authorization. So, for example, access to customer IP or MAC addresses would trigger the notification requirement, regardless of whether any sensitive information was

---

<sup>10</sup> See, e.g., Cal. Civ. Code § 1798.82(h) (defining “personal information”).

<sup>11</sup> Nevada AB 0179 (2015).

<sup>12</sup> Illinois SB 1833 (2015).

<sup>13</sup> See e.g., Kentucky HB 581 (2010).

<sup>14</sup> 47 U.S.C. § 222(h)(1).

accessed with it. Furthermore, all this information would be required to be secured by access controls and to be stored at all times behind access logs. This is an unwise mandatory allocation of security resources by critical infrastructure providers.

The NPRM's proposed information security and breach notice requirements are totally unprecedented in the United States and go far, far beyond state information security and breach notice requirements. No state breach notice law requires securing or providing breach notice about information that is simply linked or linkable to an individual, much less of IP addresses or MAC addresses. Similarly, no state law requires adopting risk management practices, strong customer authentication requirements, and maintaining year-long logs of all access to or disclosure of this broad range of information (including by or to contractors), as the NPRM proposes.

For the reasons stated at the end of the previous section, the Commission should narrow its definition in the final rule to cover only information that is sensitive and if acquired by an unauthorized person creates real risk of use on its own to harm an ISP customer. To do otherwise, would run counter to a core principle of the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, ISO security standards, the FTC security framework, and the Gramm-Leach-Bliley Act Safeguards Rule that organizations should distinguish between situations that create real risk and those that do not.

What is more, as NIST noted in its Framework for Improving Critical Infrastructure Cybersecurity,<sup>15</sup> operators must prioritize assets. Audit logging, specific security requirements and breach notification for unauthorized access to non-sensitive information would be a

---

<sup>15</sup> NIST, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), *available at* <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

distraction and inappropriate use of security resources in any sector, but is particularly unwise for critical infrastructure operators.

### **B. Notice Requirements**

The notice trigger in the NPRM proposal is a good example of the mismatch created by an extension of the current CPNI framework to broadband data. There is no harm trigger for the breach notice, unlike in 41 states. The sum-total of the NPRM proposal's requirements differ markedly from breach notice requirements under the various state laws. Unlike every state law, the proposal would require notification:

- (1) in all cases to the Commission within seven days and to individuals within 10 days,
- (2) even if the customer data were encrypted or otherwise protected;
- (3) even if an employee or contractor accidentally accessed customer information for a legitimate business purpose in excess of authorization; and
- (4) even if an employer or contractor had the right to access the system, but did so in a way that exceeded permissions in company policy.

Unlike 44 state breach laws, the NPRM proposal would require notice even if the unauthorized person simply accessed the system and did not copy or download any material from it. It would apply when there was access to garden-variety name and address information, or a broad range of information that if acquired would not itself identify an individual, such as IP addresses, MAC addresses, or information that is "linkable" to an individual, and to information that is widely available on the Internet. None of these requirements is sound information security policy.

We emphasize that because the statute says nothing at all about breach notice, all of these anomalies in the security breach notice proposal can easily be fixed in the final rule.

## **1. Absence of Any Harm Trigger**

As explained in the preceding section, a core principle of information security law and best practices is to distinguish between circumstances in which there is a risk of harm from unauthorized acquisition of data and circumstances where there is not. A large majority of state breach notice laws (41 out of 47) contain a “harm trigger” to distinguish between these circumstances and to avoid over-notification. Under the state breach notice laws, notice is typically required when acquisition of personally identifiable information creates some sort of risk of harm to individuals. Harm exists where the unauthorized acquisition creates a material or significant risk of identity theft, fraud, or in some cases, breach of very sensitive personal information such as private medical data.

The NPRM’s proposed definitions of CPNI and customer proprietary information sweep in a broad range of data that do not themselves create risk of harm if they fall into the hands of an unauthorized person.

The CPNI statute does not say anything about security requirements and does not even mention breach notice. It certainly poses no impediment to the Commission tempering the requirements of the CPNI Rule and the NPRM’s Proposed Rule to reflect risk of harm by narrowing the range of information to which audit trail and breach notice requirements apply to and by including a risk of harm trigger before notice is required.

## **2. Short-Fuse 7- and 10-Day Breach Notice Deadlines**

A 10-day notice requirement to customers is without precedent even in the current CPNI rules and does not provide businesses with nearly enough time to conduct a thorough and accurate investigation. Complicated breaches may take well over a month to investigate properly. The shortest state notice deadline to affected individuals is 30 days with a 15 day

extension,<sup>16</sup> and that law is an outlier in state data breach law. Most states have no deadline at all beyond what is “unreasonable delay,” and those that do generally provide 45 days to notify consumers after a breach has been confirmed.<sup>17</sup> Some other states with deadlines have flexible ones -- within 45 days unless a longer period of time is required to determine the scope of the breach or to prepare proper notice.<sup>18</sup>

When a breach or suspected breach occurs, a company’s top priorities are to ascertain the nature of the event, restore the security and integrity of the affected system, and determine the scope of the incident and who was affected. Time is of the essence. A requirement to report very quickly after discovery of a breach takes important resources away from remediation and investigation. What is more, in complex breaches involving hacking it can take far longer to determine the extent of the incident. Requiring notice to customers within ten days in many cases is to require incomplete or inaccurate notice. For this reason, other federal breach notice requirements, such as the Gramm-Leach-Bliley Act interagency guidance<sup>19</sup> and the HI-TECH Act amendments to HIPAA,<sup>20</sup> like the state breach notice laws, impose no deadline or a much longer deadline.

Notice would also be required to the Commission and in some cases to both the FBI and Secret Service within 7 days. While this notice requirement is in the current CPNI rules, any notice requirement, much less a short-fuse one, does not make sense as to a breach of non-sensitive information for which the FBI and Secret Service would not launch an investigation.

---

<sup>16</sup> See Fla. Stat. §501.171.

<sup>17</sup> See e.g., Ohio Rev. Code § 1347.12.

<sup>18</sup> See e.g., R.I. Gen. Laws § 11-49.2-1 *et seq.*

<sup>19</sup> E.g., 12 C.F.R. Part 208, App. D-2 (as soon as possible).

<sup>20</sup> 45 C.F.R. § 164.400-414 (60 day deadline).

Indeed, it is important to understand that *only one* of the state breach notice laws, New Jersey's, requires notice to a law enforcement investigative agency in the case of a data breach, and imposes no deadline for accomplishing this. This breach notice deadline is in no way suggested by the statute. Rather, it was adopted by the Commission in 2007, during the politically charged time of pretexting scandals. There is no valid reason for a very short deadline to notify of a breach of either CPNI or customer proprietary information.

### **3. Requiring Notice for “Access” Instead of “Acquisition” of Data**

An “access” standard is unusual. It errs on the side of over-notification. In the case of a hacking incident, an “acquisition” standard limits notification obligations to individuals whose files it is reasonable to believe that a hacker has either downloaded or viewed. (When a hacker views a file, then a copy is made to the Random Access Memory of the hacker's computer and the data have been acquired.) By contrast, the “access” term is ambiguous and may be read as requiring, for example, notice to everyone in a database if an intruder enters a database containing information about a million people, but logging reveals that the intruder only viewed 6 people's files.

Only 3 states require breach notice in cases of simple “access”, without “acquisition”, of sensitive data. All of these states -- Connecticut, New Jersey and Florida -- have a high risk of harm trigger that must be met before breach notice is required. In Florida, for example, notice is required where there has been “unauthorized access of electronic data containing personal information” but only where more than 500 Florida residents were affected.<sup>21</sup> However, the NPRM does not contain any harm trigger.

---

<sup>21</sup> See Fla. Stat. §501.171(3)(a).

Under all other state laws, not only is the breach notice law triggered when there is an *acquisition* of data, as opposed to *access* (as discussed above), there is no mandatory notice to law enforcement, with the exception of state Attorneys General in a minority of states.<sup>22</sup> The model used by almost all but two of these states requires notification to the Attorney General when residents are notified.<sup>23</sup>

#### **4. Requiring Notice for Breaches of Data that Are Unreadable or Unusable**

*Every* state breach notice law exempts from notification breaches of sensitive personal information that is encrypted. The vast majority of states also exempt from notice breaches of information that is rendered “unreadable or unusable” through any reasonable method. The NPRM proposal omits this exception, which is necessary both to avoid over-notification and to incentivize use of encryption to secure sensitive data.

#### **5. Requiring Notice in Cases of Good Faith Employee Access That Exceeds Authorized Access**

Both the existing rule and the NPRM would require notice in situations in which employees access databases containing regulated information, even if the employee does so in good faith and in the course of his or her employment.

Again, *every* state breach notice law exempts from notice situations in which employees acting in good faith view or acquire data without authorization in the course of carrying out the employees’ jobs, provided that the information is not misused or further disclosed.<sup>24</sup> This is not a data breach and it serves no purpose to require notice. Indeed, imposing a notice obligation in this situation risks having the counterproductive effect of discouraging employers from

---

<sup>22</sup> *See, e.g.*, Cal. Civ. Code §§ 1798.82.

<sup>23</sup> *See e.g.*, Cal. Civ. Code § 1798.82(f)

<sup>24</sup> *See* Ga. Code §§ 10-1-911

establishing beneficial policies against employee access to sensitive data systems, as doing so would perversely increase the risk of having to provide breach notice.

The Commission should fix this anomaly in the CPNI Rule, instead of compounding it here.

### **6. Eliminating an Intentional Access Trigger for Notice**

Whereas the current Rule requires some intentional act to trigger a notice requirement, the NPRM proposal would eliminate even that requirement. This would mean that if an employee accidentally accessed a database containing the broad range of information covered by the proposed Rule, breach notice would be required. Intentionality is no substitute for limiting data elements requiring notice to data elements that are inherently risky or for incorporating a harm trigger in the final rule, but its omission in the NPRM proposal would create even more over-notification.

## **IV. CONCLUSION**

For the reasons stated above, we respectfully urge the Commission to revise the proposed definitions of customer proprietary network information (“CPNI”) and the vast new category of customer proprietary information to focus only on *sensitive* information, and to reserve its logging and access control information security obligations and its unprecedented and extreme breach notice requirements for that sensitive information. We further urge the Commission to align its proposed breach notice requirements so that they do not exceed the longstanding requirements under state breach notice laws and to apply requirements only to knowing violations. Finally, we urge the Commission to revise its definition of de-identified data to make it fully consistent with the FTC’s definition, as applied, and remove the proposed requirement that data be *both* de-identified *and* aggregated. These changes would create a robust FCC risk-

based information security and breach notice regime that is consistent with sound data and cybersecurity practices and protective of consumers.

Respectfully submitted,

/s/

Jim Halpert  
Anne Kierig  
James Duchesne  
Counsel to the State Privacy and Security Coalition, Inc.  
DLA Piper LLP (US)  
500 8th Street, NW  
Washington, D.C. 20004  
(202) 799-4441