



July 27, 2015

The Honorable Michael C. Burgess, Chairman  
The Honorable Jan Schakowsky, Ranking Member  
Committee on Energy & Commerce  
Subcommittee on Commerce, Manufacturing, and Trade  
2125 Rayburn House Office Building  
Washington, DC 20515

Re: Additional Questions for the Record

Dear Chairman Burgess and Representative Schakowsky:

Thank you so much for providing me with the opportunity to respond to additional questions for the record regarding the Data Security and Breach Notification Act of 2015. Please note that I represent a nonprofit organization with extremely limited resources. With the very helpful assistance of our one legal intern,<sup>1</sup> we have answered the provided questions as comprehensively and accurately as possible in our best effort to provide this important public service. However, the level of legal detail required to answer the numerous questions regarding state law is beyond my capacity to fully review to my complete satisfaction on the required timeline. Therefore I cannot guarantee these responses against missed state laws or regulations or other inaccuracies, and would encourage anyone relying on the information herein to double check the citations provided. I apologize for any inconvenience this may present, but again am very grateful and honored to have had the opportunity to testify on this issue and to respond to these important questions.

Please find my responses below.

Questions from the Honorable Michael C. Burgess

1. *Which states require commercial entities to secure specific data elements, typically designated as personal information or personally identifiable information?*

---

<sup>1</sup> Many thanks to Matthew Baker, OTI's exceptional 2015 summer law student intern, who provided indispensable support researching and drafting these responses.

States that require commercial entities to secure specific data elements are Arkansas,<sup>2</sup> California,<sup>3</sup> Connecticut,<sup>4</sup> Florida,<sup>5</sup> Indiana,<sup>6</sup> Maryland,<sup>7</sup> Massachusetts,<sup>8</sup> Nevada,<sup>9</sup> Oregon,<sup>10</sup> Rhode Island,<sup>11</sup> Texas,<sup>12</sup> and Utah.<sup>13</sup>

---

<sup>2</sup> Ark. Code Ann. § 4-110-104(b) (“A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”).

<sup>3</sup> Cal. Civ. Code § 1798.81.5(b) (“A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”).

<sup>4</sup> 2015 Conn. Legis. Serv. P.A. 15-142 (S.B. 949) at (2) (“Implement and maintain a comprehensive data-security program for the protection of confidential information. The safeguards contained in such program shall be consistent with and comply with the safeguards for protection of confidential information as set forth in all applicable federal and state law and written policies of the state contained in the agreement.”).

<sup>5</sup> Fla. Stat. Ann. § 501.171(2) (“Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information.”).

<sup>6</sup> Ind. Code Ann. § 24-4.9-3-3.5(b) (“A data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.”).

<sup>7</sup> Md. Code Ann., Com. Law § 14-3503(a) (“To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations.”).

<sup>8</sup> Mass. Gen. Laws Ann. ch. 93H, § 2(a) (“The department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. Such regulations shall be designed to safeguard the personal information of residents of the commonwealth and shall be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated. The objectives of the regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to

2. *Are there any states that do not require commercial entities to secure an individual's data, typically designated as personal information or personally identifiable information? If so, please list those states.*

The remaining states do not have laws that specifically require commercial entities to secure an individual's data. Those states are: Alabama, Alaska, Arizona, Colorado, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma,

---

the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer. The regulations shall take into account the person's size, scope and type of business, the amount of resources available to such person, the amount of stored data, and the need for security and confidentiality of both consumer and employee information.”).

<sup>9</sup> Nev. Rev. Stat. Ann. § 603A.210(1) (“A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.”).

<sup>10</sup> Or. Rev. Stat. Ann. § 646A.622(1) (“Any person that owns, maintains or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including disposal of the data.”).

<sup>11</sup> R.I. Gen. Laws Ann. § 11-49.2-7 (“Any state agency or person that maintains its own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of § 11-49.2-3, shall be deemed to be in compliance with the security breach notification requirements of § 11-49.2-3, provided such person notifies subject persons in accordance with such person's policies in the event of a breach of security.”).

<sup>12</sup> Tex. Bus. & Com. Code Ann. § 521.052(a) (“A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.”).

<sup>13</sup> Utah Code Ann. § 13-44-201 (“Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and (b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person.”).

Pennsylvania, South Carolina, South Dakota, Tennessee, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

However, state Attorneys General in a number of these states have interpreted other state consumer protection laws to include a requirement that commercial entities holding personal information implement reasonable security standards to protect that information. For example, in 2014 TD Bank agreed to a settlement with a nine-state group that had sued the company for inadequate security practices. The group included states with no data security statute: Maine, New Jersey, New York, North Carolina, Pennsylvania, and Vermont.<sup>14</sup> Similarly, in 2015 Zappos.com agreed to a data security–related settlement with a multi-state group that included Arizona, Kentucky, North Carolina, Ohio, and Pennsylvania—all states with no specific data security statute.<sup>15</sup>

In addition, the Federal Trade Commission has interpreted federal law to require commercial entities in every state and territory to provide reasonable and appropriate protections for consumers’ personal information.<sup>16</sup>

3. *Please identify with a direct citation states that require a commercial entity to secure the following data elements by state statute or regulation:*
  - a. *An individual’s name, home address or telephone number, mother’s maiden name (if identified as such), and their birth data.*

---

<sup>14</sup> The states with no specific data security laws on the books nevertheless cited a number of consumer protection statutes in support of a reasonable data security requirement. TD Bank Settlement (Oct. 3, 2014), *available at* [http://www.ct.gov/ag/lib/ag/press\\_releases/2014/20141016\\_oag\\_cdp\\_tdbank\\_settlement.pdf](http://www.ct.gov/ag/lib/ag/press_releases/2014/20141016_oag_cdp_tdbank_settlement.pdf) (citing Me. Rev. Stat. tit. 5, § 207; Me. Rev. Stat. tit. 5, § 209; N.J. Stat. Ann. § 56:8-1; N.Y. Exec. Law § 63; N.Y. Gen. Bus. Law § 349; N.Y. Gen. Bus. Law § 350; N.C. Gen. Stat. Ann. § 75-1.1; 73 Pa. Cons. Stat. Ann. § 201-1; 73 Pa. Cons. Stat. Ann. § 2301; Vt. Stat. Ann. tit. 8, § 2709).

<sup>15</sup> Zappos.com Settlement (Jan. 5, 2015), *available at* [http://www.ncdoj.gov/getdoc/507c1254-6390-4635-abae-9281f58f2929/Zappo-Assurance-of-Voluntary-Compliance-\(2\).aspx](http://www.ncdoj.gov/getdoc/507c1254-6390-4635-abae-9281f58f2929/Zappo-Assurance-of-Voluntary-Compliance-(2).aspx).

<sup>16</sup> See Prepared Statement of the Federal Trade Commission on Discussion Draft of H.R. \_\_\_, Data Security and Breach Notification Act Of 2015 at 3 (Mar. 18, 2015), *available at* [https://www.ftc.gov/system/files/documents/public\\_statements/630961/150318datasecurity.pdf](https://www.ftc.gov/system/files/documents/public_statements/630961/150318datasecurity.pdf) (“Since 2001, the Commission has used its deception and unfairness authority under these laws to take enforcement action and obtain settlements in more than 50 cases against businesses that it charged with failing to provide reasonable and appropriate protections for consumers’ personal information.”).

To the best of my knowledge, there is no state statute in any state that specifically requires a commercial entity to secure these data elements.

*b. A financial account number or credit or debit card number or other identifier, in combination with any security code, access code, or password.*

States that require a commercial entity to secure these data elements by state statute or regulation are Arkansas,<sup>17</sup> California,<sup>18</sup> Florida,<sup>19</sup> Indiana,<sup>20</sup> Maryland,<sup>21</sup> Massachusetts,<sup>22</sup> Nevada,<sup>23</sup> Oregon,<sup>24</sup> Rhode Island,<sup>25</sup> Texas,<sup>26</sup> and Utah.<sup>27</sup>

*c. A unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, biometric data unique to an individual, or password that is required for an individual to obtain money, or purchase goods, services, or any other thing of value.*

To the best of my knowledge, the only state that specifically requires a commercial entity to secure these data elements by state statute or regulation is Connecticut.<sup>28</sup>

*d. A non-truncated social security number.*

States that require a commercial entity to secure this information by state statute or regulation are Arkansas,<sup>29</sup> California,<sup>30</sup> Connecticut,<sup>31</sup> Florida,<sup>32</sup> Indiana,<sup>33</sup> Maryland,<sup>34</sup> Massachusetts,<sup>35</sup> Nevada,<sup>36</sup> Oregon,<sup>37</sup> Rhode Island,<sup>38</sup> Texas,<sup>39</sup> and Utah.<sup>40</sup>

---

<sup>17</sup> Ark. Code Ann. § 4-110-104(b).

<sup>18</sup> Cal. Civ. Code § 1798.81.5.

<sup>19</sup> Fla. Stat. Ann. § 501.171.

<sup>20</sup> Ind. Code Ann. § 24-4.9-3-3.5(b).

<sup>21</sup> Md. Code Ann., Com. Law § 14-3501.

<sup>22</sup> Mass. Gen. Laws Ann. ch. 93H, § 1.

<sup>23</sup> Nev. Rev. Stat. Ann. § 603A.040.

<sup>24</sup> Or. Rev. Stat. Ann. § 646A.602.

<sup>25</sup> R.I. Gen. Laws Ann. § 11-49.2-5.

<sup>26</sup> Tex. Bus. & Com. Code Ann. § 521.002.

<sup>27</sup> Utah Code Ann. § 13-44-102.

<sup>28</sup> 2015 Conn. Legis. Serv. P.A. 15-142.

<sup>29</sup> Ark. Code Ann. § 4-110-104(b).

<sup>30</sup> Cal. Civ. Code § 1798.80.

<sup>31</sup> 2015 Conn. Legis. Serv. P.A. 15-142 (S.B. 949).

<sup>32</sup> Fla. Stat. Ann. § 501.171.

<sup>33</sup> Ind. Code Ann. § 24-4.9-3-3.5(b).

- e. *Any information that pertains to the transmission of specific calls, including for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.*

To the best of my knowledge, there are no states that require a commercial entity to secure this information by state statute or regulation. However, this information is already protected under federal law.<sup>41</sup>

- f. *A username or email address, in combination with a password or security question and answer that would permit access to an online account.*

States that require a commercial entity to secure this information by state statute or regulation are California,<sup>42</sup> Florida,<sup>43</sup> Nevada,<sup>44</sup> and Rhode Island.<sup>45</sup>

- g. *A government issued unique identification number, including driver's license number, passport number, or alien registration number.*

States that require a commercial entity to secure this information by state statute or regulation are Arkansas,<sup>46</sup> California,<sup>47</sup> Connecticut,<sup>48</sup> Florida,<sup>49</sup> Indiana,<sup>50</sup> Maryland,<sup>51</sup> Massachusetts,<sup>52</sup> Nevada,<sup>53</sup> Oregon,<sup>54</sup> Rhode Island,<sup>55</sup> and Utah.<sup>56</sup>

---

<sup>34</sup> Md. Code Ann., Com. Law § 14-3501.

<sup>35</sup> Mass. Gen. Laws Ann. ch. 93H, § 1.

<sup>36</sup> Nev. Rev. Stat. Ann. § 603A.040.

<sup>37</sup> Or. Rev. Stat. Ann. § 646A.602

<sup>38</sup> R.I. Gen. Laws Ann. § 11-49.2-5

<sup>39</sup> Tex. Bus. & Com. Code Ann. § 521.002.

<sup>40</sup> Utah Code Ann. § 13-44-102.

<sup>41</sup> 47 U.S.C. § 222; 47 CFR 64.2009; Notice of Apparent Liability and Forfeiture, *In re TerraCom, Inc. and YourTel America, Inc.* (rel. Oct. 24, 2014), available at <https://www.fcc.gov/document/10m-fine-proposed-against-terracom-and-yourtel-privacy-breaches>.

<sup>42</sup> 2015 Cal. Legis. Serv. Ch. 96 (A.B. 1541).

<sup>43</sup> Fla. Stat. Ann. § 501.171.

<sup>44</sup> 2015 Nevada Laws Ch. 55 (A.B. 179).

<sup>45</sup> 2015 Rhode Island Laws Ch. 15-138 (15-S 134B).

<sup>46</sup> Ark. Code Ann. § 4-110-104(b).

<sup>47</sup> Cal. Civ. Code § 1798.81.5.

<sup>48</sup> 2015 Conn. Legis. Serv. P.A. 15-142 (S.B. 949).

<sup>49</sup> Fla. Stat. Ann. § 501.171.

<sup>50</sup> Ind. Code Ann. § 24-4.9-3-3.5(b).

*h. An individual's name and their medical information.*

States that require a commercial entity to secure this information by state statute or regulation are Arkansas,<sup>57</sup> California,<sup>58</sup> Connecticut,<sup>59</sup> Florida,<sup>60</sup> Oregon,<sup>61</sup> Rhode Island,<sup>62</sup> and Texas.<sup>63</sup>

*i. An individual's name and their health insurance policy number, subscriber identification number, or patient number used by a health insurer to identify the individual, including any related identification number within that individual's health insurance claim appeal records.*

States that require a commercial entity to secure this information by state statute or regulation are Connecticut,<sup>64</sup> Florida,<sup>65</sup> Nevada,<sup>66</sup> Oregon,<sup>67</sup> Rhode Island,<sup>68</sup> and Texas.<sup>69</sup>

*4. Please identify with a direct citation states that require a commercial entity to provide notification to a consumer after the breach of the following data elements by state statute or regulation:*

*a. An individual's name, home address or telephone number, mother's maiden name (if identified as such), and their birth date.*

---

<sup>51</sup> Md. Code Ann., Com. Law § 14-3501.

<sup>52</sup> Mass. Gen. Laws Ann. ch. 93H, § 1.

<sup>53</sup> Nev. Rev. Stat. Ann. § 603A.040.

<sup>54</sup> Or. Rev. Stat. Ann. § 646A.602

<sup>55</sup> R.I. Gen. Laws Ann. § 11-49.2-5

<sup>56</sup> Utah Code Ann. § 13-44-102.

<sup>57</sup> Ark. Code Ann. § 4-110-104(b).

<sup>58</sup> Cal. Civ. Code § 1798.81.5.

<sup>59</sup> 2015 Conn. Legis. Serv. P.A. 15-142 (S.B. 949).

<sup>60</sup> Fla. Stat. Ann. § 501.171.

<sup>61</sup> Oregon Laws Ch. 357 (S.B. 601).

<sup>62</sup> 2015 Rhode Island Laws Ch. 15-138 (15-S 134B).

<sup>63</sup> Tex. Bus. & Com. Code Ann. § 521.002.

<sup>64</sup> 2015 Conn. Legis. Serv. P.A. 15-142 (S.B. 949).

<sup>65</sup> Fla. Stat. Ann. § 501.171.

<sup>66</sup> 2015 Nevada Laws Ch. 55 (A.B. 179).

<sup>67</sup> Oregon Laws Ch. 357 (S.B. 601).

<sup>68</sup> 2015 Rhode Island Laws Ch. 15-138 (15-S 134B).

<sup>69</sup> Tex. Bus. & Com. Code Ann. § 521.002.

To the best of my knowledge, the only state with a state statute that requires a commercial entity to provide notification to a consumer after breach of this information is Texas.<sup>70</sup>

*b. A financial account number or credit or debit card number or other identifier, in combination with any security code, access code, or password.*

States and territories with statutes that require a commercial entity to provide notification to a consumer after breach of this information are Alaska,<sup>71</sup> Arizona,<sup>72</sup> Arkansas,<sup>73</sup> California,<sup>74</sup> Colorado,<sup>75</sup> Connecticut,<sup>76</sup> Delaware,<sup>77</sup> Florida,<sup>78</sup> Georgia,<sup>79</sup> Hawaii,<sup>80</sup> Idaho,<sup>81</sup> Illinois,<sup>82</sup> Indiana,<sup>83</sup> Iowa,<sup>84</sup> Kansas,<sup>85</sup> Kentucky,<sup>86</sup> Louisiana,<sup>87</sup> Maine,<sup>88</sup> Maryland,<sup>89</sup> Massachusetts,<sup>90</sup> Michigan,<sup>91</sup> Minnesota,<sup>92</sup> Mississippi,<sup>93</sup> Missouri,<sup>94</sup> Montana,<sup>95</sup> Nebraska,<sup>96</sup> Nevada,<sup>97</sup> New Hampshire,<sup>98</sup> New Jersey,<sup>99</sup> New York,<sup>100</sup> North

---

<sup>70</sup> Tex. Bus. & Com. Code Ann. § 521.002(1).

<sup>71</sup> Alaska Stat. Ann. § 45.48.090.

<sup>72</sup> Ariz. Rev. Stat. Ann. § 44-7501.

<sup>73</sup> Ark. Code Ann. § 4-110-103.

<sup>74</sup> 2015 Cal. Legis. Serv. Ch. 96 (A.B. 1541).

<sup>75</sup> Colo. Rev. Stat. Ann. § 6-1-716.

<sup>76</sup> 2015 Conn. Legis. Serv. P.A. 15-142 (S.B. 949).

<sup>77</sup> Del. Code Ann. tit. 6, § 12B-101.

<sup>78</sup> Fla. Stat. Ann. § 501.171.

<sup>79</sup> Ga. Code Ann. § 10-1-911.

<sup>80</sup> Haw. Rev. Stat. § 487N-1.

<sup>81</sup> Idaho Code Ann. § 28-51-104.

<sup>82</sup> 815 Ill. Comp. Stat. Ann. 530/5.

<sup>83</sup> Ind. Code Ann. § 4-1-11-3.

<sup>84</sup> Iowa Code Ann. § 715C.1.

<sup>85</sup> Kan. Stat. Ann. § 50-7a01.

<sup>86</sup> Ky. Rev. Stat. Ann. § 365.732.

<sup>87</sup> La. Rev. Stat. Ann. 51:3073.

<sup>88</sup> Me. Rev. Stat. tit. 10, § 1347.

<sup>89</sup> Md. Code Ann., Com. Law § 14-3501.

<sup>90</sup> Mass. Gen. Laws Ann. ch. 93H, § 1.

<sup>91</sup> Mich. Comp. Laws Ann. § 445.63.

<sup>92</sup> Minn. Stat. Ann. § 325E.61.

<sup>93</sup> Miss. Code. Ann. § 75-24-29.

<sup>94</sup> Mo. Ann. Stat. § 407.1500.

<sup>95</sup> MT LEGIS 62 (2015), 2015 Montana Laws Ch. 62 (H.B. 74).

<sup>96</sup> Neb. Rev. Stat. § 87-802.



Dakota,<sup>101</sup> Ohio,<sup>102</sup> Oklahoma,<sup>103</sup> Oregon,<sup>104</sup> Pennsylvania,<sup>105</sup> Rhode Island,<sup>106</sup> South Carolina,<sup>107</sup> Tennessee,<sup>108</sup> Texas,<sup>109</sup> Utah,<sup>110</sup> Vermont,<sup>111</sup> Virginia,<sup>112</sup> Washington,<sup>113</sup> West Virginia,<sup>114</sup> Wisconsin,<sup>115</sup> Wyoming,<sup>116</sup> Washington, D.C.,<sup>117</sup> Guam,<sup>118</sup> Puerto Rico,<sup>119</sup> and U.S. Virgin Islands.<sup>120</sup>

- c. *A unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, biometric data unique to an individual, or password that is required for an individual to obtain money, or purchase goods, services, or any other thing of value.*

States with state statutes that require a commercial entity to provide notification to a consumer after breach of this information are Iowa,<sup>121</sup> Missouri,<sup>122</sup> Nebraska,<sup>123</sup> and Vermont.<sup>124</sup>

---

<sup>97</sup> 2015 Nevada Laws Ch. 55 (A.B. 179).

<sup>98</sup> N.H. Rev. Stat. Ann. § 359-C:19.

<sup>99</sup> N.J. Stat. Ann. § 56:8-161.

<sup>100</sup> N.Y. Gen. Bus. Law § 899-aa.

<sup>101</sup> ND LEGIS S.B. 2214 (2015).

<sup>102</sup> Ohio Rev. Code Ann. § 1349.19.

<sup>103</sup> Okla. Stat. Ann. tit. 24, § 162.

<sup>104</sup> Oregon Laws Ch. 357 (S.B. 601).

<sup>105</sup> 73 Pa. Cons. Stat. Ann. § 2302.

<sup>106</sup> Rhode Island Laws Ch. 15-138 (15-S 134B).

<sup>107</sup> S.C. Code Ann. § 39-1-90.

<sup>108</sup> Tenn. Code Ann. § 47-18-2107.

<sup>109</sup> Tex. Bus. & Com. Code Ann. § 521.002.

<sup>110</sup> Utah Code Ann. § 13-44-102.

<sup>111</sup> Vt. Stat. Ann. tit. 9, § 2430.

<sup>112</sup> Va. Code Ann. § 18.2-186.6.

<sup>113</sup> Wash. Legis. Serv. Ch. 64 (S.H.B. 1078).

<sup>114</sup> W. Va. Code Ann. § 46A-2A-101.

<sup>115</sup> Wis. Stat. Ann. § 134.98.

<sup>116</sup> Wyo. Stat. Ann. § 6-3-901.

<sup>117</sup> D.C. Code § 28-3851.

<sup>118</sup> 9 G.C.A. § 48.20.

<sup>119</sup> 10 L.P.R.A. § 4051.

<sup>120</sup> 14 V.I.C. § 2208.

<sup>121</sup> Iowa Code Ann. § 715C.1.

<sup>122</sup> Mo. Ann. Stat. § 407.1500.

*d. A non-truncated social security number.*

States and territories with statutes that require a commercial entity to provide notification to a consumer after breach of this information are Alaska,<sup>125</sup> Arizona,<sup>126</sup> Arkansas,<sup>127</sup> California,<sup>128</sup> Colorado,<sup>129</sup> Connecticut,<sup>130</sup> Delaware,<sup>131</sup> Florida,<sup>132</sup> Georgia,<sup>133</sup> Hawaii,<sup>134</sup> Idaho,<sup>135</sup> Illinois,<sup>136</sup> Indiana,<sup>137</sup> Iowa,<sup>138</sup> Kansas,<sup>139</sup> Kentucky,<sup>140</sup> Louisiana,<sup>141</sup> Maine,<sup>142</sup> Maryland,<sup>143</sup> Massachusetts,<sup>144</sup> Michigan,<sup>145</sup> Minnesota,<sup>146</sup> Mississippi,<sup>147</sup> Missouri,<sup>148</sup> Montana,<sup>149</sup> Nebraska,<sup>150</sup> Nevada,<sup>151</sup> New Hampshire,<sup>152</sup> New Jersey,<sup>153</sup> New

---

<sup>123</sup> Neb. Rev. Stat. § 87-802.

<sup>124</sup> Vt. Stat. Ann. tit. 9, § 2430.

<sup>125</sup> Alaska Stat. Ann. § 45.48.090.

<sup>126</sup> Ariz. Rev. Stat. Ann. § 44-7501.

<sup>127</sup> Ark. Code Ann. § 4-110-103.

<sup>128</sup> 2015 Cal. Legis. Serv. Ch. 96 (A.B. 1541).

<sup>129</sup> Colo. Rev. Stat. Ann. § 6-1-716.

<sup>130</sup> 2015 Conn. Legis. Serv. P.A. 15-142 (S.B. 949).

<sup>131</sup> Del. Code Ann. tit. 6, § 12B-101.

<sup>132</sup> Fla. Stat. Ann. § 501.171.

<sup>133</sup> Ga. Code Ann. § 10-1-911.

<sup>134</sup> Haw. Rev. Stat. § 487N-1.

<sup>135</sup> Idaho Code Ann. § 28-51-104.

<sup>136</sup> 815 Ill. Comp. Stat. Ann. 530/5.

<sup>137</sup> Ind. Code Ann. § 4-1-11-3.

<sup>138</sup> Iowa Code Ann. § 715C.1.

<sup>139</sup> Kan. Stat. Ann. § 50-7a01.

<sup>140</sup> Ky. Rev. Stat. Ann. § 365.732.

<sup>141</sup> La. Rev. Stat. Ann. 51:3073.

<sup>142</sup> Me. Rev. Stat. tit. 10, § 1347.

<sup>143</sup> Md. Code Ann., Com. Law § 14-3501.

<sup>144</sup> Mass. Gen. Laws Ann. ch. 93H, § 1.

<sup>145</sup> Mich. Comp. Laws Ann. § 445.63.

<sup>146</sup> Minn. Stat. Ann. § 325E.61.

<sup>147</sup> Miss. Code. Ann. § 75-24-29.

<sup>148</sup> Mo. Ann. Stat. § 407.1500.

<sup>149</sup> MT LEGIS 62 (2015), 2015 Montana Laws Ch. 62 (H.B. 74).

<sup>150</sup> Neb. Rev. Stat. § 87-802.

<sup>151</sup> 2015 Nevada Laws Ch. 55 (A.B. 179).

<sup>152</sup> N.H. Rev. Stat. Ann. § 359-C:19.

<sup>153</sup> N.J. Stat. Ann. § 56:8-161.

York,<sup>154</sup> North Carolina,<sup>155</sup> North Dakota,<sup>156</sup> Ohio,<sup>157</sup> Oklahoma,<sup>158</sup> Oregon,<sup>159</sup> Pennsylvania,<sup>160</sup> Rhode Island,<sup>161</sup> South Carolina,<sup>162</sup> Tennessee,<sup>163</sup> Texas,<sup>164</sup> Utah,<sup>165</sup> Vermont,<sup>166</sup> Virginia,<sup>167</sup> Washington,<sup>168</sup> West Virginia,<sup>169</sup> Wisconsin,<sup>170</sup> Wyoming,<sup>171</sup> Washington, D.C.,<sup>172</sup> Guam,<sup>173</sup> Puerto Rico,<sup>174</sup> and U.S. Virgin Islands.<sup>175</sup>

- e. *Any information that pertains to the transmission of specific calls, including for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.*

To the best of my knowledge, there are no states that require a commercial entity to secure this information by state statute or regulation. However, federal law already requires telecommunications carriers to provide notification to a consumer after breach of this information.<sup>176</sup>

- f. *A user name or email address, in combination with a password or security question and answer that would permit access to an online account.*

---

<sup>154</sup> N.Y. Gen. Bus. Law § 899-aa.

<sup>155</sup> N.C. Gen. Stat. Ann. § 14-113.20 (West 2005)

<sup>156</sup> ND LEGIS S.B. 2214 (2015).

<sup>157</sup> Ohio Rev. Code Ann. § 1349.19.

<sup>158</sup> Okla. Stat. Ann. tit. 24, § 162.

<sup>159</sup> Oregon Laws Ch. 357 (S.B. 601).

<sup>160</sup> 73 Pa. Cons. Stat. Ann. § 2302.

<sup>161</sup> Rhode Island Laws Ch. 15-138 (15-S 134B).

<sup>162</sup> S.C. Code Ann. § 39-1-90.

<sup>163</sup> Tenn. Code Ann. § 47-18-2107.

<sup>164</sup> Tex. Bus. & Com. Code Ann. § 521.002.

<sup>165</sup> Utah Code Ann. § 13-44-102.

<sup>166</sup> Vt. Stat. Ann. tit. 9, § 2430.

<sup>167</sup> Va. Code Ann. § 18.2-186.6.

<sup>168</sup> Wash. Legis. Serv. Ch. 64 (S.H.B. 1078).

<sup>169</sup> W. Va. Code Ann. § 46A-2A-101.

<sup>170</sup> Wis. Stat. Ann. § 134.98.

<sup>171</sup> Wyo. Stat. Ann. § 6-3-901.

<sup>172</sup> D.C. Code § 28-3851.

<sup>173</sup> 9 G.C.A. § 48.20.

<sup>174</sup> 10 L.P.R.A. § 4051.

<sup>175</sup> 14 V.I.C. § 2208.

<sup>176</sup> 47 CFR 64.2011; 47 U.S.C. § 222.

States and territories with statutes that require a commercial entity to provide notification to a consumer after breach of this information are California,<sup>177</sup> Florida,<sup>178</sup> Nevada,<sup>179</sup> Rhode Island,<sup>180</sup> Wyoming,<sup>181</sup> and Puerto Rico.<sup>182</sup>

- g. A government issued unique identification number, including driver's license number, passport number, or alien registration number.*

States and territories with statutes that require a commercial entity to provide notification to a consumer after breach of this information are Alaska,<sup>183</sup> Arizona,<sup>184</sup> Arkansas,<sup>185</sup> California,<sup>186</sup> Colorado,<sup>187</sup> Connecticut,<sup>188</sup> Delaware,<sup>189</sup> Florida,<sup>190</sup> Georgia,<sup>191</sup> Hawaii,<sup>192</sup> Idaho,<sup>193</sup> Illinois,<sup>194</sup> Indiana,<sup>195</sup> Iowa,<sup>196</sup> Kansas,<sup>197</sup> Kentucky,<sup>198</sup> Louisiana,<sup>199</sup> Maine,<sup>200</sup> Maryland,<sup>201</sup> Massachusetts,<sup>202</sup> Michigan,<sup>203</sup> Minnesota,<sup>204</sup> Mississippi,<sup>205</sup>

---

<sup>177</sup> 2015 Cal. Legis. Serv. Ch. 96 (A.B. 1541).

<sup>178</sup> Fla. Stat. Ann. § 501.171.

<sup>179</sup> 2015 Nevada Laws Ch. 55 (A.B. 179).

<sup>180</sup> Rhode Island Laws Ch. 15-138 (15-S 134B).

<sup>181</sup> Wyo. Stat. Ann. § 6-3-901.

<sup>182</sup> 10 L.P.R.A. § 4051.

<sup>183</sup> Alaska Stat. Ann. § 45.48.090.

<sup>184</sup> Ariz. Rev. Stat. Ann. § 44-7501.

<sup>185</sup> Ark. Code Ann. § 4-110-103.

<sup>186</sup> 2015 Cal. Legis. Serv. Ch. 96 (A.B. 1541).

<sup>187</sup> Colo. Rev. Stat. Ann. § 6-1-716.

<sup>188</sup> 2015 Conn. Legis. Serv. P.A. 15-142 (S.B. 949).

<sup>189</sup> Del. Code Ann. tit. 6, § 12B-101.

<sup>190</sup> Fla. Stat. Ann. § 501.171.

<sup>191</sup> Ga. Code Ann. § 10-1-911.

<sup>192</sup> Haw. Rev. Stat. § 487N-1.

<sup>193</sup> Idaho Code Ann. § 28-51-104.

<sup>194</sup> 815 Ill. Comp. Stat. Ann. 530/5.

<sup>195</sup> Ind. Code Ann. § 4-1-11-3.

<sup>196</sup> Iowa Code Ann. § 715C.1.

<sup>197</sup> Kan. Stat. Ann. § 50-7a01.

<sup>198</sup> Ky. Rev. Stat. Ann. § 365.732.

<sup>199</sup> La. Rev. Stat. Ann. 51:3073.

<sup>200</sup> Me. Rev. Stat. tit. 10, § 1347.

<sup>201</sup> Md. Code Ann., Com. Law § 14-3501.

<sup>202</sup> Mass. Gen. Laws Ann. ch. 93H, § 1.

<sup>203</sup> Mich. Comp. Laws Ann. § 445.63.

<sup>204</sup> Minn. Stat. Ann. § 325E.61.

Missouri,<sup>206</sup> Montana,<sup>207</sup> Nebraska,<sup>208</sup> Nevada,<sup>209</sup> New Hampshire,<sup>210</sup> New Jersey,<sup>211</sup> New York,<sup>212</sup> North Carolina,<sup>213</sup> North Dakota,<sup>214</sup> Ohio,<sup>215</sup> Oklahoma,<sup>216</sup> Oregon,<sup>217</sup> Pennsylvania,<sup>218</sup> Rhode Island,<sup>219</sup> South Carolina,<sup>220</sup> Tennessee,<sup>221</sup> Texas,<sup>222</sup> Utah,<sup>223</sup> Vermont,<sup>224</sup> Virginia,<sup>225</sup> Washington,<sup>226</sup> West Virginia,<sup>227</sup> Wisconsin,<sup>228</sup> Wyoming,<sup>229</sup> Washington, D.C.,<sup>230</sup> Guam,<sup>231</sup> Puerto Rico,<sup>232</sup> and U.S. Virgin Islands.<sup>233</sup>

*h. An individual's name and their medical information.*

States and territories with statutes that require a commercial entity to provide notification to a consumer after breach of this information are Arkansas,<sup>234</sup> California,<sup>235</sup>

---

<sup>205</sup> Miss. Code. Ann. § 75-24-29.

<sup>206</sup> Mo. Ann. Stat. § 407.1500.

<sup>207</sup> MT LEGIS 62 (2015), 2015 Montana Laws Ch. 62 (H.B. 74).

<sup>208</sup> Neb. Rev. Stat. § 87-802.

<sup>209</sup> 2015 Nevada Laws Ch. 55 (A.B. 179).

<sup>210</sup> N.H. Rev. Stat. Ann. § 359-C:19.

<sup>211</sup> N.J. Stat. Ann. § 56:8-161.

<sup>212</sup> N.Y. Gen. Bus. Law § 899-aa.

<sup>213</sup> N.C. Gen. Stat. Ann. § 14-113.20 (West 2005)

<sup>214</sup> ND LEGIS S.B. 2214 (2015).

<sup>215</sup> Ohio Rev. Code Ann. § 1349.19.

<sup>216</sup> Okla. Stat. Ann. tit. 24, § 162.

<sup>217</sup> Oregon Laws Ch. 357 (S.B. 601).

<sup>218</sup> 73 Pa. Cons. Stat. Ann. § 2302.

<sup>219</sup> Rhode Island Laws Ch. 15-138 (15-S 134B).

<sup>220</sup> S.C. Code Ann. § 39-1-90.

<sup>221</sup> Tenn. Code Ann. § 47-18-2107.

<sup>222</sup> Tex. Bus. & Com. Code Ann. § 521.002.

<sup>223</sup> Utah Code Ann. § 13-44-102.

<sup>224</sup> Vt. Stat. Ann. tit. 9, § 2430.

<sup>225</sup> Va. Code Ann. § 18.2-186.6.

<sup>226</sup> Wash. Legis. Serv. Ch. 64 (S.H.B. 1078).

<sup>227</sup> W. Va. Code Ann. § 46A-2A-101.

<sup>228</sup> Wis. Stat. Ann. § 134.98.

<sup>229</sup> Wyo. Stat. Ann. § 6-3-901.

<sup>230</sup> D.C. Code § 28-3851.

<sup>231</sup> 9 G.C.A. § 48.20.

<sup>232</sup> 10 L.P.R.A. § 4051.

<sup>233</sup> 14 V.I.C. § 2208.

<sup>234</sup> Ark. Code Ann. § 4-110-103.

Florida,<sup>236</sup> Michigan,<sup>237</sup> Missouri,<sup>238</sup> Montana,<sup>239</sup> Nevada,<sup>240</sup> Rhode Island,<sup>241</sup> Texas,<sup>242</sup> Wyoming,<sup>243</sup> and Puerto Rico.<sup>244</sup>

- i. *An individual's name and their health insurance policy number, subscriber identification number, or patient number used by a health insurer to identify the individual, including any related identification number within that individual's health insurance claim appeal records.*

States with statutes that require a commercial entity to provide notification to a consumer after breach of this information are California,<sup>245</sup> Connecticut,<sup>246</sup> Florida,<sup>247</sup> Michigan,<sup>248</sup> Missouri,<sup>249</sup> Nevada,<sup>250</sup> Rhode Island,<sup>251</sup> Texas,<sup>252</sup> and Wyoming,<sup>253</sup>

#### Questions from the Honorable Jan Schakowsky

1. *Section 6(c)(2) of the draft bill appears to try to limit the preemption of certain sections of the Communications Act and related regulations to the extent that they apply to data security and breach notification. But those provisions of the Communications Act also provide for broader privacy protections.*
  - a. *Do you agree that there is no simple distinction between privacy and data security? Why is it so difficult to separate privacy and data security?*

---

<sup>235</sup> 2015 Cal. Legis. Serv. Ch. 96 (A.B. 1541).

<sup>236</sup> Fla. Stat. Ann. § 501.171.

<sup>237</sup> Mich. Comp. Laws Ann. § 445.63.

<sup>238</sup> Mo. Ann. Stat. § 407.1500.

<sup>239</sup> MT LEGIS 62 (2015), 2015 Montana Laws Ch. 62 (H.B. 74).

<sup>240</sup> 2015 Nevada Laws Ch. 55 (A.B. 179).

<sup>241</sup> Rhode Island Laws Ch. 15-138 (15-S 134B).

<sup>242</sup> Tex. Bus. & Com. Code Ann. § 521.002.

<sup>243</sup> Wyo. Stat. Ann. § 6-3-901.

<sup>244</sup> 10 L.P.R.A. § 4051.

<sup>245</sup> 2015 Cal. Legis. Serv. Ch. 96 (A.B. 1541).

<sup>246</sup> 2015 Conn. Legis. Serv. P.A. 15-142 (S.B. 949).

<sup>247</sup> Fla. Stat. Ann. § 501.171.

<sup>248</sup> Mich. Comp. Laws Ann. § 445.63.

<sup>249</sup> Mo. Ann. Stat. § 407.1500.

<sup>250</sup> 2015 Nevada Laws Ch. 55 (A.B. 179).

<sup>251</sup> Rhode Island Laws Ch. 15-138 (15-S 134B).

<sup>252</sup> Tex. Bus. & Com. Code Ann. § 521.002.

<sup>253</sup> Wyo. Stat. Ann. § 6-3-901.

I agree that there is no simple distinction between privacy and data security. When a data breach occurs, the consumer whose personal information has been compromised finds that both her privacy and the security of her data have been violated. As I explained in my written testimony,

We generally think of “privacy” as having to do with how information flows, what flows are appropriate, and who gets to make those determinations. Data or information “security” refers to the tools used to ensure that information flows occur as intended. When a data breach occurs, both the subject’s privacy (his right to control how his information is used or shared) and information security (the measures put in place to facilitate and protect that control) are violated.

Privacy and security are thus distinct concepts, but they go hand in hand. From the consumer’s perspective, a data breach that results in the exposure of her call records to the world is a terrible violation of her privacy. But the cause of the privacy violation may be a breakdown in security.

Indeed, agencies enforcing against entities for security failures cite both privacy and security at the same time. For example:

- In the April 8, 2015 Order issued by the Federal Communications Commission adopting a Consent Decree to resolve its investigation into AT&T’s “fail[ure] to properly protect the confidentiality of almost 280,000 customers’ proprietary information, . . . in connection with data breaches at AT&T call centers in Mexico, Columbia, and the Philippines,” the FCC explained that “AT&T will be required to improve its *privacy* and data security practices by appointing a senior compliance manager who is *privacy certified*, conducting a *privacy risk assessment*, implementing an information security program, preparing an appropriate compliance manual, and regularly training employees on the company’s *privacy policies* and the applicable *privacy legal authorities*.”<sup>254</sup>
- In the complaint it filed in June 2010 against Twitter for failing to implement reasonable security, the Federal Trade Commission argued that Twitter had “failed to provide reasonable and appropriate security to: prevent unauthorized access to

---

<sup>254</sup> *AT&T Services, Inc.*, Order, para. 2 (2015), available at [http://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2015/db0408/DA-15-399A1.pdf](http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0408/DA-15-399A1.pdf) (emphasis added) [hereinafter AT&T Order].

nonpublic user information *and honor the privacy choices exercised by its users in designating certain tweets as nonpublic.*"<sup>255</sup>

*b. What are the consequences of the preemption of the Communications Act being open to broad interpretation?*

The difficulty of drawing a bright line distinction between privacy and security is a cause for concern under the bill because the bill supersedes several sections of the Communications Act to the extent those sections “apply to covered entities with respect to securing information in electronic form from unauthorized access, including notification of unauthorized access to data in electronic form containing personal information.” Some have interpreted this language to mean that the bill would not interfere with privacy-related rules and enforcement actions adopted by the Federal Communications Commission. But if privacy and security cannot be clearly distinguished, the bill threatens to supersede much, if not all, of the FCC’s privacy jurisdiction and related rules.

*c. Even if this preemption does leave the privacy protections intact, will there be difficulties for the FCC to regulate and enforce those privacy protections? Please explain?*

Yes, even if this preemption leaves privacy protections intact, the FCC will have a difficult time regulating and enforcing privacy protections. That’s because even regulatory and enforcement actions that are arguably purely privacy-related will be subject to challenges. For example, the FCC has a rule that states:

If a telecommunications carrier provides different categories of service, but a customer does not subscribe to more than one offering by the carrier, the carrier is not permitted to share [customer proprietary network information, or] CPNI with its affiliates, except as provided in §64.2007(b).<sup>256</sup>

This is a privacy rule, because it governs the control that carriers must provide their customers over the customers’ private information. Thus the FCC would likely retain this rule even if the bill were to pass.

But in the event that a carrier later shared information between its affiliates without customer consent in violation of this rule, and the FCC enforced the rule, the

---

<sup>255</sup> *Twitter, Inc.*, Complaint, para. 11 (2010), available at <https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100624twittercmpt.pdf> (emphasis added).

<sup>256</sup> 47 C.F.R. § 64.2005(a)(2).



violator might challenge the rule or enforcement under this bill. Although the rule at issue governs specific circumstances when the carrier must get the customer's permission to share CPNI, the carrier could argue that its violation of the rule, resulting in unauthorized sharing of the CPNI between affiliates, concerned a failure to "secur[e] information in electronic form from unauthorized access," and that the FCC therefore had no jurisdiction to enforce the privacy rule against it under this set of circumstances.

Uncertainty regarding the FCC's authority to regulate and enforce consumer privacy protections could handicap the agency, and could ultimately result in the high costs of mounting legal defenses against challenges.

- d. In your written testimony, you gave an example regarding the recent news of permacookies/supercookies, describing how Verizon, or another company, could exploit those regulation and enforcement difficulties to avoid enforcement altogether. Can you expand on that example?*

Once broadband access service is reclassified as a telecommunications service under Title II of the Communications Act, § 222 of the Communications Act, governing the privacy and security of CPNI, will apply to Internet service providers (ISPs). Under its § 222 authority, the FCC could determine that broadband customers' browsing histories constitute CPNI, and that ISPs must not disclose their customers' browsing histories without customer consent.

In the Verizon permacookie example, a tool created by Verizon to power its own advertising efforts was found to be useable by other advertisers who wanted to track Verizon customers' browsing patterns. Indeed, *ProPublica* reported in January that online ad company Turn was in fact using the permacookie for that purpose.<sup>257</sup>

After reclassification becomes effective, the FCC could bring an enforcement action against an ISP for failing to get consent before injecting something like the permacookie into customers' Web traffic, because the permacookie arguably "disclose[d]" customers' browsing histories. But under this bill, the ISP could challenge the enforcement, arguing that it had not gotten customer consent for the permacookie because it only intended the permacookie to be used for internal purposes, and that the fact that the permacookie could be used by an advertiser to reveal an individual customer's browsing history was due to the ISP's inadvertent failure to "secur[e] information in electronic form from unauthorized access."

---

<sup>257</sup> Julia Angwin & Mike Tigas, *Zombie Cookie: The Tracking Cookie That You Can't Kill*, *ProPublica* (Jan. 14, 2015), <https://www.propublica.org/article/zombie-cookie-the-tracking-cookie-that-you-cant-kill>.

Not only would such a challenge jeopardize the FCC’s ability to protect consumers against an enormous privacy threat, but it would call into question the ability of any regulator at all to protect against the threat. Browsing history does not fall under this bill’s definition of personal information. Therefore the FTC could not respond to the permacookie as a data breach. Nor could the FTC enforce against the ISP using its general authority to prohibit “unfair or deceptive acts or practices” under § 5 of the FTC Act, because the FTC’s authority under that section does not extend to telecommunications carriers.<sup>258</sup>

2. *In your written testimony, you raised concerns that certain types of information that is required to be secured under the Communications Act and associated regulations would not be required to be secured under the discussion draft. Please provide some specific examples of the types of information that are currently required to be secured under the Communications Act, with reference to the specific statute and/or regulation, that would no longer be required to be secured under the discussion draft.*

Among the sections of the Communications Act that would be limited by this bill are 222, 338, and 631 (47 U.S.C. §§ 222, 338, and 551), which govern the privacy and security of telecommunications, satellite, and cable, respectively. The following chart compares the information that is currently protected under each of these three sections with what would be protected under the bill:

Relevant Section of Communications Act	Information Required to Be Secured Under Existing Federal Law	Protected Under this Bill?
222 (47 U.S.C. § 222)	the location of, number from which and to which a call is placed, and the time and duration of such call	yes
	the location of, number from which and to which a text message is sent, and the time of such text message	no
	other “information that relates 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 that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship”	no
	“information contained in the bills	no

---

<sup>258</sup> 15 U.S.C. § 45.

	pertaining to telephone exchange service or telephone toll service received by a customer of a carrier”	
	information about a customer’s use of broadband access service (after Title II reclassification becomes effective)	no
338 (47 U.S.C. § 338)	satellite customers’ viewing and order histories	no
631 (47 U.S.C. § 551)	cable customers’ viewing and order histories	no

As is clear from the chart, the vast majority of information that is currently required to be secured under the Communications Act would no longer be required to be secured if this bill passed. If this bill passed, consumers could lose vital security protections for sensitive information such as:

- A web browsing history that reveals visits to several websites describing Alzheimer’s disease—its symptoms, diagnosis, and treatment, as well as websites providing resources and emotional support for Alzheimer’s sufferers and their family members.
  - A text message history that reveals a large volume of text messages exchanged between two individuals suspected of having an affair.
  - A video on demand history that reveals several late-night orders of adult films.
  - Broadband access records that reveal with great precision when a customer is at home and when she is out.
3. *We have heard multiple times that this discussion draft has nothing to do with net neutrality and the reclassification of broadband internet access under Title II. However, if this discussion draft were enacted, it would affect the FCC’s data security authority over internet service providers.*
- a. *How might Sections 201, 202, and 222 of the Communications Act and the associated regulations be applied to broadband internet access with regard to data security and breach notification when the new open internet rules go into effect?*

When the new rules go into effect and broadband access service is reclassified as a telecommunications service under Title II of the Communications Act, provisions of Title II that protect customers’ personal information and that protect them from unjust and unreasonable practices will apply to Internet service providers (ISPs). This includes § 222, which requires telecommunications providers to protect the confidentiality of CPNI.

It is not yet clear how the FCC will apply these sections to ISPs, but we may look to existing FCC guidance and regulations to help predict what might happen. Currently, the FCC requires telecommunications carriers to exercise reasonable security practices to protect customers' information, and requires prompt disclosure of breaches.<sup>259</sup>

The FCC will likely also require reasonable security measures to protect customers' information, and prompt disclosure of breaches, as applied to ISPs.

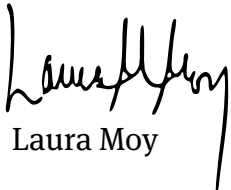
*b. Please provide some examples of the types of information related to broadband internet access that will be required to be secured under Title II and associated regulations that will not be covered by the discussion draft.*

It is unknown exactly how CPNI will be defined in the broadband context, but the FCC could find that CPNI includes information such as a customer's web browsing history, details about what devices a customer uses to connect to the Internet and when and where he uses those devices, and what applications a customer uses.

---

I hope these responses are useful to you—thank you again for the opportunity to provide them. Please do not hesitate to contact me with any additional questions.

Sincerely,



Laura Moy

---

<sup>259</sup> See AT&T Order, *supra* note 253.



April 9, 2015

Congresswoman Jan Schakowsky  
2367 Rayburn HOB  
Washington, DC 20515

Re: Additional Questions for the Record

Dear Representative Schakowsky:

Thank you so much for providing me with the opportunity to respond to additional questions for the record regarding the Data Security and Breach Notification Act of 2015. Please find my responses below.

1. *Section 6(c)(2) of the draft bill appears to try to limit the preemption of certain sections of the Communications Act and related regulations to the extent that they apply to data security and breach notification. But those provisions of the Communications Act also provide for broader privacy protections.*
  - a. *Do you agree that there is no simple distinction between privacy and data security? Why is it so difficult to separate privacy and data security?*

I agree that there is no simple distinction between privacy and data security. When a data breach occurs, the consumer whose personal information has been compromised finds that both her privacy and the security of her data have been violated. As I explained in my written testimony,

We generally think of “privacy” as having to do with how information flows, what flows are appropriate, and who gets to make those determinations. Data or information “security” refers to the tools used to ensure that information flows occur as intended. When a data breach occurs, both the subject’s privacy (his right to control how his information is used or shared) and information security (the measures put in place to facilitate and protect that control) are violated.

Privacy and security are thus distinct concepts, but they go hand in hand. From the consumer’s perspective, a data breach that results in the exposure of her call records to the world is a terrible violation of her privacy. But the cause of the privacy violation may be a breakdown in security.

Indeed, agencies enforcing against entities for security failures cite both privacy and security at the same time. For example:

- In the April 8, 2015 Order issued by the Federal Communications Commission adopting a Consent Decree to resolve its investigation into AT&T’s “fail[ure] to properly protect the confidentiality of almost 280,000 customers’ proprietary information, . . . in connection with data breaches at AT&T call centers in Mexico, Columbia, and the Philippines,” the FCC explained that “AT&T will be required to improve its *privacy* and data security practices by appointing a senior compliance manager who is *privacy certified*, conducting a *privacy risk assessment*, implementing an information security program, preparing an appropriate compliance manual, and regularly training employees on the company’s *privacy policies* and the applicable *privacy legal authorities*.”<sup>1</sup>
- In the complaint it filed in June 2010 against Twitter for failing to implement reasonable security, the Federal Trade Commission argued that Twitter had “failed to provide reasonable and appropriate security to: prevent unauthorized access to nonpublic user information *and honor the privacy choices exercised by its users in designating certain tweets as nonpublic*.”<sup>2</sup>

b. *What are the consequences of the preemption of the Communications Act being open to broad interpretation?*

The difficulty of drawing a bright line distinction between privacy and security is a cause for concern under the bill because the bill supersedes several sections of the Communications Act to the extent those sections “apply to covered entities with respect to securing information in electronic form from unauthorized access, including notification of unauthorized access to data in electronic form containing personal information.” Some have interpreted this language to mean that the bill would not interfere with privacy-related rules and enforcement actions adopted by the Federal

---

<sup>1</sup> *AT&T Services, Inc.*, Order, para. 2 (2015), available at [http://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2015/db0408/DA-15-399A1.pdf](http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0408/DA-15-399A1.pdf) (emphasis added) [hereinafter AT&T Order].

<sup>2</sup> *Twitter, Inc.*, Complaint, para. 11 (2010), available at <https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100624twittercmpt.pdf> (emphasis added).

Communications Commission. But if privacy and security cannot be clearly distinguished, the bill threatens to supersede much, if not all, of the FCC's privacy jurisdiction and related rules.

- c. Even if this preemption does leave the privacy protections intact, will there be difficulties for the FCC to regulate and enforce those privacy protections? Please explain?*

Yes, even if this preemption leaves privacy protections intact, the FCC will have a difficult time regulating and enforcing privacy protections. That's because even regulatory and enforcement actions that are arguably purely privacy-related will be subject to challenges. For example, the FCC has a rule that states:

If a telecommunications carrier provides different categories of service, but a customer does not subscribe to more than one offering by the carrier, the carrier is not permitted to share [customer proprietary network information, or] CPNI with its affiliates, except as provided in §64.2007(b).<sup>3</sup>

This is a privacy rule, because it governs the control that carriers must provide their customers over the customers' private information. Thus the FCC would likely retain this rule even if the bill were to pass.

But in the event that a carrier later shared information between its affiliates without customer consent in violation of this rule, and the FCC enforced the rule, the violator might challenge the rule or enforcement under this bill. Although the rule at issue governs specific circumstances when the carrier must get the customer's permission to share CPNI, the carrier could argue that its violation of the rule, resulting in unauthorized sharing of the CPNI between affiliates, concerned a failure to "secur[e] information in electronic form from unauthorized access," and that the FCC therefore had no jurisdiction to enforce the privacy rule against it under this set of circumstances.

Uncertainty regarding the FCC's authority to regulate and enforce consumer privacy protections could handicap the agency, and could ultimately result in the high costs of mounting legal defenses against challenges.

- d. In your written testimony, you gave an example regarding the recent news of permacookies/supercookies, describing how Verizon, or another company, could exploit those regulation*

---

<sup>3</sup> 47 C.F.R. § 64.2005(a)(2).

*and enforcement difficulties to avoid enforcement altogether.  
Can you expand on that example?*

Once broadband access service is reclassified as a telecommunications service under Title II of the Communications Act, § 222 of the Communications Act, governing the privacy and security of CPNI, will apply to Internet service providers (ISPs). Under its § 222 authority, the FCC could determine that broadband customers' browsing histories constitute CPNI, and that ISPs must not disclose their customers' browsing histories without customer consent.

In the Verizon permacookie example, a tool created by Verizon to power its own advertising efforts was found to be useable by other advertisers who wanted to track Verizon customers' browsing patterns. Indeed, *ProPublica* reported in January that online ad company Turn was in fact using the permacookie for that purpose.<sup>4</sup>

After reclassification becomes effective, the FCC could bring an enforcement action against an ISP for failing to get consent before injecting something like the permacookie into customers' Web traffic, because the permacookie arguably "disclose[d]" customers' browsing histories. But under this bill, the ISP could challenge the enforcement, arguing that it had not gotten customer consent for the permacookie because it only intended the permacookie to be used for internal purposes, and that the fact that the permacookie could be used by an advertiser to reveal an individual customer's browsing history was due to the ISP's inadvertent failure to "secur[e] information in electronic form from unauthorized access."

Not only would such a challenge jeopardize the FCC's ability to protect consumers against an enormous privacy threat, but it would call into question the ability of any regulator at all to protect against the threat. Browsing history does not fall under this bill's definition of personal information. Therefore the FTC could not respond to the permacookie as a data breach. Nor could the FTC enforce against the ISP using its general authority to prohibit "unfair or deceptive acts or practices" under § 5 of the FTC Act, because the FTC's authority under that section does not extend to telecommunications carriers.<sup>5</sup>

- 2. In your written testimony, you raised concerns that certain types of information that is required to be secured under the Communications Act and associated regulations would not be required to be secured*

---

<sup>4</sup> Julia Angwin & Mike Tigas, *Zombie Cookie: The Tracking Cookie That You Can't Kill*, *ProPublica* (Jan. 14, 2015), <https://www.propublica.org/article/zombie-cookie-the-tracking-cookie-that-you-cant-kill>.

<sup>5</sup> 15 U.S.C. § 45.



*under the discussion draft. Please provide some specific examples of the types of information that are currently required to be secured under the Communications Act, with reference to the specific statute and/or regulation, that would no longer be required to be secured under the discussion draft.*

Among the sections of the Communications Act that would be limited by this bill are 222, 338, and 631 (47 U.S.C. §§ 222, 338, and 551), which govern the privacy and security of telecommunications, satellite, and cable, respectively. The following chart compares the information that is currently protected under each of these three sections with what would be protected under the bill:

Relevant Section of Communications Act	Information Required to Be Secured Under Existing Federal Law	Protected Under this Bill?
222 (47 U.S.C. § 222)	the location of, number from which and to which a call is placed, and the time and duration of such call	yes
	the location of, number from which and to which a text message is sent, and the time of such text message	no
	other “information that relates 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 that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship”	no
	“information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier”	no
	information about a customer’s use of broadband access service (after Title II reclassification becomes effective)	no
338 (47 U.S.C. § 338)	satellite customers’ viewing and order histories	no
631 (47 U.S.C. § 551)	cable customers’ viewing and order histories	no

As is clear from the chart, the vast majority of information that is currently required to be secured under the Communications Act would no longer be required to be secured if this bill passed. If this bill passed,

consumers could lose vital security protections for sensitive information such as:

- A web browsing history that reveals visits to several websites describing Alzheimer’s disease—its symptoms, diagnosis, and treatment, as well as websites providing resources and emotional support for Alzheimer’s sufferers and their family members.
  - A text message history that reveals a large volume of text messages exchanged between two individuals suspected of having an affair.
  - A video on demand history that reveals several late-night orders of adult films.
  - Broadband access records that reveal with great precision when a customer is at home and when she is out.
3. *We have heard multiple times that this discussion draft has nothing to do with net neutrality and the reclassification of broadband internet access under Title II. However, if this discussion draft were enacted, it would affect the FCC’s data security authority over internet service providers.*
- a. *How might Sections 201, 202, and 222 of the Communications Act and the associated regulations be applied to broadband internet access with regard to data security and breach notification when the new open internet rules go into effect?*

When the new rules go into effect and broadband access service is reclassified as a telecommunications service under Title II of the Communications Act, provisions of Title II that protect customers’ personal information and that protect them from unjust and unreasonable practices will apply to Internet service providers (ISPs). This includes § 222, which requires telecommunications providers to protect the confidentiality of CPNI.

It is not yet clear how the FCC will apply these sections to ISPs, but we may look to existing FCC guidance and regulations to help predict what might happen. Currently, the FCC requires telecommunications carriers to exercise reasonable security practices to protect customers’ information, and requires prompt disclosure of breaches.<sup>6</sup>

The FCC will likely also require reasonable security measures to protect customers’ information, and prompt disclosure of breaches, as applied to ISPs.

---

<sup>6</sup> See AT&T Order, *supra* note 1.

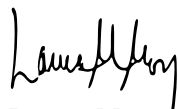
- b. *Please provide some examples of the types of information related to broadband internet access that will be required to be secured under Title II and associated regulations that will not be covered by the discussion draft.*

It is unknown exactly how CPNI will be defined in the broadband context, but the FCC could find that CPNI includes information such as a customer's web browsing history, details about what devices a customer uses to connect to the Internet and when and where he uses those devices, and what applications a customer uses.

---

I hope these responses are useful to you—thank you again for the opportunity to provide them. Please do not hesitate to contact me with any additional questions.

Sincerely,



Laura Moy



April 9, 2015

Congresswoman Jan Schakowsky  
2367 Rayburn HOB  
Washington, DC 20515

Re: Additional Questions for the Record

Dear Representative Schakowsky:

Thank you so much for providing me with the opportunity to respond to additional questions for the record regarding the Data Security and Breach Notification Act of 2015. Please find my responses below.

1. *Section 6(c)(2) of the draft bill appears to try to limit the preemption of certain sections of the Communications Act and related regulations to the extent that they apply to data security and breach notification. But those provisions of the Communications Act also provide for broader privacy protections.*
  - a. *Do you agree that there is no simple distinction between privacy and data security? Why is it so difficult to separate privacy and data security?*

I agree that there is no simple distinction between privacy and data security. When a data breach occurs, the consumer whose personal information has been compromised finds that both her privacy and the security of her data have been violated. As I explained in my written testimony,

We generally think of “privacy” as having to do with how information flows, what flows are appropriate, and who gets to make those determinations. Data or information “security” refers to the tools used to ensure that information flows occur as intended. When a data breach occurs, both the subject’s privacy (his right to control how his information is used or shared) and information security (the measures put in place to facilitate and protect that control) are violated.

Privacy and security are thus distinct concepts, but they go hand in hand. From the consumer’s perspective, a data breach that results in the exposure of her call records to the world is a terrible violation of her privacy. But the cause of the privacy violation may be a breakdown in security.

Indeed, agencies enforcing against entities for security failures cite both privacy and security at the same time. For example:

- In the April 8, 2015 Order issued by the Federal Communications Commission adopting a Consent Decree to resolve its investigation into AT&T’s “fail[ure] to properly protect the confidentiality of almost 280,000 customers’ proprietary information, . . . in connection with data breaches at AT&T call centers in Mexico, Columbia, and the Philippines,” the FCC explained that “AT&T will be required to improve its *privacy* and data security practices by appointing a senior compliance manager who is *privacy certified*, conducting a *privacy risk assessment*, implementing an information security program, preparing an appropriate compliance manual, and regularly training employees on the company’s *privacy policies* and the applicable *privacy legal authorities*.”<sup>1</sup>
- In the complaint it filed in June 2010 against Twitter for failing to implement reasonable security, the Federal Trade Commission argued that Twitter had “failed to provide reasonable and appropriate security to: prevent unauthorized access to nonpublic user information *and honor the privacy choices exercised by its users in designating certain tweets as nonpublic*.”<sup>2</sup>

b. *What are the consequences of the preemption of the Communications Act being open to broad interpretation?*

The difficulty of drawing a bright line distinction between privacy and security is a cause for concern under the bill because the bill supersedes several sections of the Communications Act to the extent those sections “apply to covered entities with respect to securing information in electronic form from unauthorized access, including notification of unauthorized access to data in electronic form containing personal information.” Some have interpreted this language to mean that the bill would not interfere with privacy-related rules and enforcement actions adopted by the Federal

---

<sup>1</sup> *AT&T Services, Inc.*, Order, para. 2 (2015), available at [http://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2015/db0408/DA-15-399A1.pdf](http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0408/DA-15-399A1.pdf) (emphasis added) [hereinafter AT&T Order].

<sup>2</sup> *Twitter, Inc.*, Complaint, para. 11 (2010), available at <https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100624twittercmpt.pdf> (emphasis added).

Communications Commission. But if privacy and security cannot be clearly distinguished, the bill threatens to supersede much, if not all, of the FCC's privacy jurisdiction and related rules.

- c. Even if this preemption does leave the privacy protections intact, will there be difficulties for the FCC to regulate and enforce those privacy protections? Please explain?*

Yes, even if this preemption leaves privacy protections intact, the FCC will have a difficult time regulating and enforcing privacy protections. That's because even regulatory and enforcement actions that are arguably purely privacy-related will be subject to challenges. For example, the FCC has a rule that states:

If a telecommunications carrier provides different categories of service, but a customer does not subscribe to more than one offering by the carrier, the carrier is not permitted to share [customer proprietary network information, or] CPNI with its affiliates, except as provided in §64.2007(b).<sup>3</sup>

This is a privacy rule, because it governs the control that carriers must provide their customers over the customers' private information. Thus the FCC would likely retain this rule even if the bill were to pass.

But in the event that a carrier later shared information between its affiliates without customer consent in violation of this rule, and the FCC enforced the rule, the violator might challenge the rule or enforcement under this bill. Although the rule at issue governs specific circumstances when the carrier must get the customer's permission to share CPNI, the carrier could argue that its violation of the rule, resulting in unauthorized sharing of the CPNI between affiliates, concerned a failure to "secur[e] information in electronic form from unauthorized access," and that the FCC therefore had no jurisdiction to enforce the privacy rule against it under this set of circumstances.

Uncertainty regarding the FCC's authority to regulate and enforce consumer privacy protections could handicap the agency, and could ultimately result in the high costs of mounting legal defenses against challenges.

- d. In your written testimony, you gave an example regarding the recent news of permacookies/supercookies, describing how Verizon, or another company, could exploit those regulation*

---

<sup>3</sup> 47 C.F.R. § 64.2005(a)(2).

*and enforcement difficulties to avoid enforcement altogether.  
Can you expand on that example?*

Once broadband access service is reclassified as a telecommunications service under Title II of the Communications Act, § 222 of the Communications Act, governing the privacy and security of CPNI, will apply to Internet service providers (ISPs). Under its § 222 authority, the FCC could determine that broadband customers' browsing histories constitute CPNI, and that ISPs must not disclose their customers' browsing histories without customer consent.

In the Verizon permacookie example, a tool created by Verizon to power its own advertising efforts was found to be useable by other advertisers who wanted to track Verizon customers' browsing patterns. Indeed, *ProPublica* reported in January that online ad company Turn was in fact using the permacookie for that purpose.<sup>4</sup>

After reclassification becomes effective, the FCC could bring an enforcement action against an ISP for failing to get consent before injecting something like the permacookie into customers' Web traffic, because the permacookie arguably "disclose[d]" customers' browsing histories. But under this bill, the ISP could challenge the enforcement, arguing that it had not gotten customer consent for the permacookie because it only intended the permacookie to be used for internal purposes, and that the fact that the permacookie could be used by an advertiser to reveal an individual customer's browsing history was due to the ISP's inadvertent failure to "secur[e] information in electronic form from unauthorized access."

Not only would such a challenge jeopardize the FCC's ability to protect consumers against an enormous privacy threat, but it would call into question the ability of any regulator at all to protect against the threat. Browsing history does not fall under this bill's definition of personal information. Therefore the FTC could not respond to the permacookie as a data breach. Nor could the FTC enforce against the ISP using its general authority to prohibit "unfair or deceptive acts or practices" under § 5 of the FTC Act, because the FTC's authority under that section does not extend to telecommunications carriers.<sup>5</sup>

- 2. In your written testimony, you raised concerns that certain types of information that is required to be secured under the Communications Act and associated regulations would not be required to be secured*

---

<sup>4</sup> Julia Angwin & Mike Tigas, *Zombie Cookie: The Tracking Cookie That You Can't Kill*, *ProPublica* (Jan. 14, 2015), <https://www.propublica.org/article/zombie-cookie-the-tracking-cookie-that-you-cant-kill>.

<sup>5</sup> 15 U.S.C. § 45.

*under the discussion draft. Please provide some specific examples of the types of information that are currently required to be secured under the Communications Act, with reference to the specific statute and/or regulation, that would no longer be required to be secured under the discussion draft.*

Among the sections of the Communications Act that would be limited by this bill are 222, 338, and 631 (47 U.S.C. §§ 222, 338, and 551), which govern the privacy and security of telecommunications, satellite, and cable, respectively. The following chart compares the information that is currently protected under each of these three sections with what would be protected under the bill:

Relevant Section of Communications Act	Information Required to Be Secured Under Existing Federal Law	Protected Under this Bill?
222 (47 U.S.C. § 222)	the location of, number from which and to which a call is placed, and the time and duration of such call	yes
	the location of, number from which and to which a text message is sent, and the time of such text message	no
	other “information that relates 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 that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship”	no
	“information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier”	no
	information about a customer’s use of broadband access service (after Title II reclassification becomes effective)	no
338 (47 U.S.C. § 338)	satellite customers’ viewing and order histories	no
631 (47 U.S.C. § 551)	cable customers’ viewing and order histories	no

As is clear from the chart, the vast majority of information that is currently required to be secured under the Communications Act would no longer be required to be secured if this bill passed. If this bill passed,



consumers could lose vital security protections for sensitive information such as:

- A web browsing history that reveals visits to several websites describing Alzheimer’s disease—its symptoms, diagnosis, and treatment, as well as websites providing resources and emotional support for Alzheimer’s sufferers and their family members.
  - A text message history that reveals a large volume of text messages exchanged between two individuals suspected of having an affair.
  - A video on demand history that reveals several late-night orders of adult films.
  - Broadband access records that reveal with great precision when a customer is at home and when she is out.
3. *We have heard multiple times that this discussion draft has nothing to do with net neutrality and the reclassification of broadband internet access under Title II. However, if this discussion draft were enacted, it would affect the FCC’s data security authority over internet service providers.*
- a. *How might Sections 201, 202, and 222 of the Communications Act and the associated regulations be applied to broadband internet access with regard to data security and breach notification when the new open internet rules go into effect?*

When the new rules go into effect and broadband access service is reclassified as a telecommunications service under Title II of the Communications Act, provisions of Title II that protect customers’ personal information and that protect them from unjust and unreasonable practices will apply to Internet service providers (ISPs). This includes § 222, which requires telecommunications providers to protect the confidentiality of CPNI.

It is not yet clear how the FCC will apply these sections to ISPs, but we may look to existing FCC guidance and regulations to help predict what might happen. Currently, the FCC requires telecommunications carriers to exercise reasonable security practices to protect customers’ information, and requires prompt disclosure of breaches.<sup>6</sup>

The FCC will likely also require reasonable security measures to protect customers’ information, and prompt disclosure of breaches, as applied to ISPs.

---

<sup>6</sup> See AT&T Order, *supra* note 1.

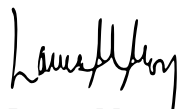
- b. *Please provide some examples of the types of information related to broadband internet access that will be required to be secured under Title II and associated regulations that will not be covered by the discussion draft.*

It is unknown exactly how CPNI will be defined in the broadband context, but the FCC could find that CPNI includes information such as a customer's web browsing history, details about what devices a customer uses to connect to the Internet and when and where he uses those devices, and what applications a customer uses.

---

I hope these responses are useful to you—thank you again for the opportunity to provide them. Please do not hesitate to contact me with any additional questions.

Sincerely,



Laura Moy