

ONE HUNDRED FOURTEENTH CONGRESS
Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

July 13, 2015

Ms. Laura Moy
Senior Policy Counsel
Open Technology Institute
New America
1899 L Street, N.W. Suite 400
Washington, D.C. 20036

Dear Ms. Moy,

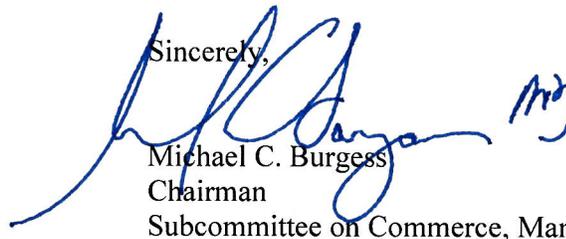
Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Wednesday, March 18, 2015, to testify at the hearing entitled "Discussion Draft of H.R. ____, Data Security and Breach Notification Act of 2015."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Monday, July 27, 2015. Your responses should be mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to Kirby.Howard@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Michael C. Burgess
Chairman
Subcommittee on Commerce, Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment

Additional Questions for the Record

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?
 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.
 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 date.
 - b. A financial account number or credit or debit card number or other identifier, in combination with any security code, access code, or password.
 - 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.
 - d. A non-truncated social security number.
 - 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.
 - 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.
 - g. A government-issued unique identification number, including driver's license number, passport number, or alien registration number.
 - h. An individual's name and their medical information.
 - 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.
 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.
- b. A financial account number or credit or debit card number or other identifier, in combination with any security code, access code, or password.
- 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.
- d. A non-truncated social security number.
- 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.
- 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.
- g. A government-issued unique identification number, including driver's license number, passport number, or alien registration number.
- h. An individual's name and their medical information.
- 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.

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

- 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?
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.
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?
 - 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.