

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1 {York Stenographic Services, Inc.}

2 RPTS BROWN

3 HIF077.170

4 DISCUSSION DRAFT OF H.R. \_\_\_\_\_, THE DATA SECURITY AND BREACH

5 NOTIFICATION ACT OF 2015

6 WEDNESDAY, MARCH 18, 2015

7 House of Representatives,

8 Subcommittee on Commerce, Manufacturing, and Trade

9 Committee on Energy and Commerce

10 Washington, D.C.

11 The Subcommittee met, pursuant to call, at 10:02 a.m.,

12 in Room 2123 of the Rayburn House Office Building, Hon.

13 Michael Burgess [Chairman of the Subcommittee] presiding.

14 Members present: Representatives Burgess, Lance,

15 Blackburn, Harper, Olson, Pompeo, Kinzinger, Bilirakis,

16 Brooks, Mullin, Upton (ex officio), Schakowsky, Clarke,

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

17 Kennedy, Cardenas, Rush, Butterfield, Welch, and Pallone (ex  
18 officio).

19 Also present: Representative McNerney.

20 Staff present: Charlotte Baker, Deputy Communications  
21 Director; Leighton Brown, Press Assistant; Karen Christian,  
22 General Counsel; James Decker, Policy Coordinator, Commerce,  
23 Manufacturing, and Trade; Graham Dufault, Counsel, Commerce,  
24 Manufacturing, and Trade; Melissa Froelich, Counsel,  
25 Commerce, Manufacturing, and Trade; Howard Kirby, Legislative  
26 Clerk; Paul Nagle, Chief Counsel, Commerce, Manufacturing,  
27 and Trade; Olivia Trusty, Professional Staff, Commerce,  
28 Manufacturing, and Trade; Michelle Ash, Democratic Chief  
29 Counsel, Commerce, Manufacturing, and Trade; Christine  
30 Brennan, Democratic Press Secretary; Jeff Carroll, Democratic  
31 Staff Director; David Goldman, Democratic Chief Counsel,  
32 Communications and Technology; Lisa Goldman, Democratic  
33 Counsel; Brendan Hennessey, Democratic Policy and Research  
34 Advisor; and Tim Robinson, Democratic Chief Counsel.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

35           Mr. {Burgess.} Chair will recognize himself for the  
36 purpose of a 5-minute opening statement. Again, welcome.  
37 Today's legislative hearing is the first concrete step for  
38 this Subcommittee toward the goal of a single Federal  
39 standard on data security and breach notification. In  
40 January we heard testimony about the key elements of sound  
41 data security and breach notification. I am pleased that so  
42 many of the elements discussed at that hearing have been  
43 incorporated into the draft legislation.

44           I also know, and I am aware of, that we just had another  
45 data breach that was in the news. I hope that the Committee  
46 looks at health care data. Health care data has its own set  
47 of policy issues, where, if sharing data is done properly,  
48 could have tremendous public benefits and save lives, but  
49 there is already law in this area under HIPAA, and taking on  
50 health care privacy data in this bill I feel would delay the  
51 consumer benefits that we can provide under this draft.

52           I am very encouraged by the bipartisan approach and  
53 commitment shown by my colleagues, Vice Chairman and full  
54 Committee Congress--the Vice Chairman of the full Committee,

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

55 Congressman Blackburn, and Congressman Welch, announcing this  
56 draft legislation. This Subcommittee has a history of  
57 bipartisan cooperation with the work of Congressman Barton  
58 and Congressman Rush, that they have put a lot into this  
59 issue over the years. I am encouraged that this may be the  
60 year that we find the paths forward.

61         The issue of data breach has been before this  
62 Subcommittee for a decade, and it is in reference to that  
63 that this is such important work. I would just acknowledge  
64 the work of previous subcommittee Chairs on both sides of the  
65 dais who have worked in this space. Chairman Bono Mack is  
66 here with us in the audience this morning. I heard from  
67 former Chairman Terry yesterday in the--on the eve of  
68 starting this hearing. And certain Chairman Rush, when I was  
69 in the minority and on this subcommittee, I know put in a lot  
70 of work.

71         But all the while that we have been working,  
72 cybercriminals have continued their operations. They steal,  
73 they monetize an individual's personal information, all of  
74 that being done in the absence of any national data security  
75 requirement. Even today the great majority of states do not

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

76 have a data security requirement. 10 years in, we do have  
77 greater insight into what cybercriminals are doing, and the  
78 impact of their activities. Conservative estimates put  
79 cybercrime cost to the consumers at \$100 billion annually,  
80 and cybercrime is estimated to cost the United States economy  
81 over a half million jobs each year.

82         The Secret Service tells us that data breaches are  
83 primarily monetized through financial fraud. On average, a  
84 third of data breach notification recipients became the  
85 victims of identity fraud in 2013, compared with a quarter in  
86 2012, clearly increasing. On a more personal level,  
87 individuals are hit twice when there is a data breach. First  
88 they need to understand which of their accounts they need to  
89 reset, if they need new bank cards, or if they need to freeze  
90 their credit report. Luckily, there are many laws to help  
91 navigate the process.

92         Second, the cost across the ecosystem is \$100 billion  
93 annually, and that is eventually passed on to the consumer in  
94 the form of higher fees and prices. The existing patchwork  
95 of state laws on data security and breach notification do not  
96 seem to have been effective. The noted security blogger

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

97 Brian Krebs posted an article this week about the new  
98 criminal tools to steal customers' payment information, and  
99 he ended it with a simple question, are online merchants  
100 ready for the coming e-commerce fraud wave? The draft  
101 legislation before us this morning addresses this question  
102 with both a security requirement for personal information  
103 that leads to identity theft and payment fraud, and a breach  
104 notification for consumers so consumers can protect  
105 themselves.

106 Some will complain about what is not in the bill. If we  
107 actually want to pass legislation, it will be impossible to  
108 proof it against what can happen in the future. We cannot  
109 shade into areas such as privacy. The--this Administration,  
110 and our minority colleagues, over the past 6 years have  
111 worked on this, and still can't agree on how to address  
112 privacy, and I just want to be very clear on that topic.  
113 While we don't tackle privacy in this legislation, we don't  
114 preempt it either. This bill is focused on unauthorized  
115 access that leads to identity theft and financial fraud. It  
116 has nothing to do with permitted access, or when that  
117 permission can be given, or what data can be collected. I

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

118 will also say that Congress must continue to address privacy  
119 of all kinds, but not at the price of delaying consumer  
120 protections for data security and breach notification.

121 Another complaint will be around moving the  
122 telecommunications, cable, and satellite providers from the  
123 Federal Communications Commission to the Federal Trade  
124 Commission. I look forward to hearing which agency has been  
125 more active--the more active consumer watchdog regarding data  
126 security and breach notification in the last 10 years.

127 I certainly do look forward to continuing the bipartisan  
128 good faith negotiations with all interested stakeholders.  
129 Negotiation remains open and ongoing, and, of course, the  
130 doors of the Subcommittee are always open.

131 [The prepared statement of Mr. Burgess follows:]

132 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

133 Mr. {Burgess.} With that, I would like to recognize the  
134 ranking member of the Subcommittee, Ms. Schakowsky, 5 minutes  
135 for an opening statement.

136 Ms. {Schakowsky.} Thank you, Mr. Chairman. I  
137 appreciate the hearing today on the draft legislation  
138 released last week, and--by Mr. Welch and Ms. Blackburn to  
139 require data breach security and reporting. I do appreciate  
140 my colleagues' efforts on this legislation, and I agree that  
141 there are some positive elements, FTC penalty authority and a  
142 data security provision among them.

143 That said, however, this bill does need significant  
144 amendments to achieve the goal of both simplifying compliance  
145 for business, and enhancing protections for consumers. I  
146 don't believe that goal is out of reach. I don't think that  
147 it expands the time that it will take. Maybe by just a bit,  
148 but the draft proposal would--has these problems, in my view.  
149 It would prevent states from enforcing their own laws related  
150 to data security and breach notification. It prevents all  
151 private rights of action on data breach and notification. As  
152 currently drafted, it would override all common law,



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

153 including tort and contract law, as they apply to data.

154 Those provisions would leave consumers with fewer protections  
155 than they currently have.

156         This proposal also weakens existing consumer protections  
157 under the Communications Act for customers of  
158 telecommunications, satellite, and cable companies. And  
159 while I believe the FTC can, and should, be empowered to play  
160 a stronger role in protecting consumers' data, I don't  
161 believe that should come at a cost of eliminating existing  
162 FCC protections. The bill would also only require consumers  
163 to be notified of a breach if it is determined that a breach  
164 has, or will, likely lead to financial harm. That would only  
165 occur after the companies regulated under this bill have  
166 concluded investigations of breaches to determine the risk of  
167 financial harm to each of their customers or users, a process  
168 that could take months.

169         There are many types of harm that go beyond simply  
170 financial ones. For example, a data breach that revealed  
171 private communication might not have any measurable financial  
172 impact, but could cause embarrassment, or even danger. The  
173 types of personal information covered by this bill are far

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

174 too limited. The bill doesn't cover over the counter drug  
175 purchases, or other health information not covered by HIPAA.  
176 By contrast, the data laws in Texas and Florida protect those  
177 types of information. The bill does not cover metadata,  
178 which can be used to acquire sensitive personal information.  
179 The bill also does not provide FTC rulemaking authority for  
180 defining personal information. This is a major weakness when  
181 we have seen the nature of personal information change  
182 significantly over time. For example, when the House passed  
183 the Data Act in 2009, it did not include geolocation  
184 information as part of personal information. Today I think  
185 we could all agree that geolocation information should be  
186 protected, and that is why we need legislation that allows  
187 the FTC to adapt as the nature of personal information  
188 continues to evolve. Of course we can't anticipate  
189 everything, but we could create some flexibility.

190 In closing, this bill is very broad, in terms of  
191 preemption of state and other Federal laws, and narrow in  
192 terms of definitions of harm and personal information. I  
193 believe the bill should be narrow where it is now broad, and  
194 broad where it is now narrow. I look forward to hearing from

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

195 our witnesses about their perspectives on this bill, and to  
196 moving forward with a strong bill that adequately protects  
197 consumers.

198 With that, I yield the remainder of my time to Mr.  
199 Kennedy.

200 [The prepared statement of Ms. Schakowsky follows:]

201 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

202           Mr. {Kennedy.} Thank you very much to my colleague, and  
203 thank you for--my colleagues on both sides of the aisle for  
204 their efforts in pulling this bill together. It is always  
205 nice to see a Bay Stater here to testify before the  
206 Committee, so I just wanted to give a warm welcome to Sara  
207 Cable, Massachusetts Assistant Attorney General with the  
208 Consumer Protection Division. Ms. Cable investigates and  
209 prosecutes violations of the Massachusetts Consumer  
210 Protections Act and the Massachusetts data notification laws  
211 and data security regulations. I have no doubt that the work  
212 that Ms. Cable does in enforcing Massachusetts data breach  
213 laws has protected many across the Commonwealth, and I truly  
214 appreciate her being willing to be here today and take some  
215 time to share her thoughts and expertise with us about an  
216 incredibly important issue.

217           And with that, Ms. Schakowsky, I will yield back. Thank  
218 you.

219           [The prepared statement of Mr. Kennedy follows:]

220 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

221           Mr. {Burgess.} Chair thanks the gentlelady. Gentlelady  
222 yields back. The Chair now recognizes the Chairman of the  
223 full Committee, Mr. Upton, 5 minutes for an opening  
224 statement.

225           The {Chairman.} Well, thank you. We are at a critical  
226 point for consumer protection in the U.S. Our interconnected  
227 economy, with many great benefits, also poses new threats  
228 from thieves, new challenges to information security, that is  
229 for sure. And as the Internet weaves itself into the DNA of  
230 appliances, cars, clothing, the threats of exploitation  
231 multiply, but the most serious underlying criminal purpose  
232 remains the same, to steal and monetize personal information,  
233 and it has to be stopped.

234           As data breaches have evolved, the one constant is that  
235 identity theft and payment card fraud are the crimes that pay  
236 the criminals. According to the Bureau of Justice  
237 Statistics, personal identity theft costs our economy nearly  
238 \$25 billion in '12, making it the largest threat to personal  
239 property today. There is not a single member of this  
240 Committee who doesn't represent someone who has suffered

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

241 either identity theft or payment fraud.

242 This bipartisan draft legislation that we consider today  
243 establishes a reasonable national security standard, with  
244 flexibility to adapt to changing security technology. The  
245 FTC and the State Attorney Generals will be policing  
246 companies to hold them accountable for protecting consumers.  
247 The draft also focuses on the personal information that  
248 criminals have targeted, the cyber gold that attracts today's  
249 cyber safecrackers. I want to thank my colleagues Blackburn  
250 and Welch for bringing us a big step closer to a bipartisan  
251 solution. Other members of the Committee, including Mr.  
252 Barton and Rush, have also rolled up their legislative  
253 sleeves over the years. And I want to thank Chairman Burgess  
254 for making this issue a very top priority on this  
255 Subcommittee.

256 I also commend the narrow approach. By targeting the  
257 most sought after personal information in the areas lacking  
258 current Federal protections, this bill avoids controversial  
259 issues that have derailed past efforts. Our goal is to  
260 create clear requirements to secure personal information  
261 from, and notify consumers in cases of unauthorized access.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

262 The goal is not to broadly regulate the use of data.

263 I yield the balance of my time to Ms. Blackburn.

264 [The prepared statement of Mr. Upton follows:]

265 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

266           Mrs. {Blackburn.} I thank the Chairman for yielding,  
267 and I also want to recognize the previous Chairman of this  
268 Committee, Ms. Bono, with us today, who have worked so  
269 diligently on this issue through the years. I appreciate the  
270 guidance and the leadership there. I also want to commend  
271 Mr. Welch, who has been co-Chairman of the Privacy Working  
272 Group, and the Chairman for allowing the Privacy Working  
273 Group a full 2 years to dig into this issue, and to see where  
274 we could find agreement. And that is the basis of the draft  
275 legislation that we have before us today.

276           The reason it is important that we do something now is  
277 because 2014 was dubbed the year of the breach. Think about  
278 the number of breaches that were out there. Our constituents  
279 have begun to see this firsthand. It has affected someone in  
280 nearly every family. And what they are saying is the issue  
281 is getting out of control, and we need to take steps to put  
282 the guidance in place so that individuals will know they have  
283 the tools that are necessary to protect their data, and, as I  
284 say, their virtual you, their presence online.

285           And I appreciate Mr. Welch and the work he and the



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

286 Privacy Working Group did to help us come to this point, and  
287 I yield the balance of my time to the gentleman from Vermont.

288 [The prepared statement of Mrs. Blackburn follows:]

289 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

290           Mr. {Welch.} Congress hasn't been doing its job. We  
291 need to pass legislation that is going to deal with this  
292 incredible problem. You know, since 2005 a billion consumer  
293 records have been hacked into. The current status right now,  
294 we have got states trying to do something. 47 different  
295 state laws on notice, 12 state laws on data security, but we  
296 don't have any national standard, and we don't have any  
297 legislative authority for the FTC, or really, for that  
298 matter, the FCC to do much, so we have to act and let there  
299 be a cop on the beat to protect people.

300           What this bill does--and this is a discussion draft, and  
301 I appreciate the back and forth, but we are going to have to  
302 have Mr. Pallone and Ms. Schakowsky very much involved as we  
303 go forward. What this does, it gives--it is a narrow bill.  
304 In my view, that is smart, because we have got to solve a  
305 problem. It gives the FTC explicit statutory authority, and  
306 that is being litigated in the Wyndham Hotels case. They can  
307 impose robust civil penalties. That is good. It does  
308 preempt states, but it doesn't limit the states with respect  
309 the states, but it doesn't limit states on privacy issues,

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

310 where they want to continue having legislative interaction.

311       This bill does not do some things that would be  
312 controversial that are debatable, but should not be part of  
313 this, because it will weigh it down. It is not a privacy  
314 bill. The states have continued authority in that space. It  
315 is not a bill about net neutrality. Big debate on this panel  
316 about the recent order. I happen to support it. Many of my  
317 colleagues don't. This bill is not about that. This bill is  
318 not about the common law right of action under tort law.  
319 Again, a debate here, but not something that we want to weigh  
320 this bill down.

321       Mr. Chairman, I appreciate the focus, the narrow focus  
322 on this. I appreciate Jan Schakowsky, the opportunity you  
323 gave me to work with the Privacy Group, and I implore all of  
324 my colleagues here to keep this going. We had good input  
325 from all of the affected parties, the FTC, the FCC consumer  
326 groups. We have got to get something done, and we have got  
327 an opportunity in this Committee to do it. I hope we can all  
328 be part of that.

329       I yield back.

330       [The prepared statement of Mr. Welch follows:]

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

331 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

332 Mr. {Burgess.} Chair thanks the gentlemen, gentleman  
333 yields back. The Chair recognizes the Ranking Member of the  
334 full Committee, Mr. Pallone, 5 minutes for an opening  
335 statement.

336 Mr. {Pallone.} Thank you, Chairman Burgess. Today we  
337 are discussing a draft data security and breach notification  
338 bill released recently by the majority. Data breaches are a  
339 plague on consumers, businesses, and our economy as a whole.  
340 Reducing the incidences of breaches, and the adverse effects  
341 from them, has rightfully been at the top of our agenda since  
342 2005, yet it also has proven to be a complicated issue,  
343 without an easy legislative solution. I appreciate the  
344 efforts being taken to address the data breach problem, and I  
345 appreciate the difficulty of writing legislation that  
346 effectively protects consumers and lessens the burdens on the  
347 businesses that are victims of criminal breaches.

348 And while the sincerity of the efforts are not  
349 questioned, I do question the merits of the bill before us  
350 today. The bill simply does not strike the right balance.  
351 There are clearly benefits to creating a unified system for

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

352 breach notification, but we must be careful that a Federal  
353 law ensures that protections for consumers are not being  
354 weakened. Many of the 51 state and territorial breach  
355 notification laws provide greater protections for consumers  
356 whose personal information is at risk as a result of data  
357 breach. For example, at least seven states and D.C. do not  
358 require a harm analysis before providing notice to consumers.  
359 At least 17 state laws also include a private cause of  
360 action. At least nine states' laws cover health information.

361 In contrast, the draft under discussion today preempts  
362 stronger state and Federal laws, requires a financial harm  
363 analysis, preempts state private rights of action, and does  
364 not cover health or location information. Data breach  
365 notification is only part of the solution. The other crucial  
366 piece of any legislation should be baseline data security to  
367 help prevent breaches before consumers' personal information  
368 is put at risk. The draft before us eliminates state data  
369 security laws and replaces them with an unclear standard that  
370 will surely be litigated and left to judicial interpretation.

371 As I said at a hearing this past January, I want to be  
372 supportive of sound data security and breach notification

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

373 legislation, but to get there we must ask the right question.  
374 The question is not whether any one Federal agency would be  
375 better off. The question must always be whether legislation  
376 puts consumers in a better place than they are today. And,  
377 unfortunately, the draft before us today does not put  
378 consumers in a better place, in my opinion.

379         So before I close, I have to raise a process issue. We  
380 received the draft bill last Thursday evening. The 114th  
381 Congress seems to have halted a long tradition of sharing  
382 text with all members of the subcommittee at least a full  
383 week prior to a legislative hearing, and this is not the  
384 first time this has happened this year in the Energy and  
385 Commerce Committee, as we saw with our Communications  
386 Subcommittee. I suspect it is not going to be the last.

387         Also, I have to take issue--I know this may sound, you  
388 know, a little picky, but I have to take issue with Chairman  
389 Burgess's opening remarks, and repeat my longstanding belief  
390 that having some Democratic support does not make a measure  
391 bipartisan. I think that Chairman Upton used better language  
392 when he said maybe it is a step closer to being bipartisan.  
393 And I appreciate what Mr. Welch said, which is that--he

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

394 mentioned having the support of myself and Ms. Schakowsky on  
395 a bill. I would like to see this bill improved before it  
396 moves further through the legislative process so that all  
397 members of the Committee can support it, and it can be a  
398 truly bipartisan legislative product, which it is not at this  
399 time.

400 I have some time left. I don't know if--did you want  
401 additional time? Are you--all right. Yvette, or--everybody  
402 is okay? All right. Thank you, Mr. Chairman. I will yield  
403 back the balance of my time.

404 [The prepared statement of Mr. Pallone follows:]

405 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

406           Mr. {Burgess.} Gentleman yields back. His observation  
407 is noted. I do want to welcome all of our witnesses, and  
408 thank you for agreeing to testify before the Committee--  
409 Subcommittee today. Today's hearing will consist of two  
410 panels. Each panel of witnesses will have the opportunity to  
411 give an opening statement, followed by a round of questions  
412 from our members. Once we conclude with questions for the  
413 first panel, we will take a brief break to set up for the  
414 second panel.

415           For our first panel today, we have the following  
416 witnesses. Ms. Jessica Rich, Director of the Bureau of  
417 Consumer Protection at the Federal Trade Commission, and Mr.  
418 Clete Johnson, the Chief Counsel for Cybersecurity, Public  
419 Safety, and Homeland Security at the Federal Communications  
420 Commission. Thank you for your participation today. Ms.  
421 Rich, you are recognized for 5 minutes for the purpose of an  
422 opening statement.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

423 ^STATEMENTS OF THE HONORABLE JESSICA RICH, DIRECTOR, BUREAU  
424 OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; AND CLETE  
425 JOHNSON, CHIEF COUNSEL FOR CYBERSECURITY, PUBLIC SAFETY AND  
426 HOMELAND SECURITY BUREAU, FEDERAL COMMUNICATIONS COMMISSION

|

427 ^STATEMENT OF JESSICA RICH

428 } Ms. {Rich.} Dr. Burgess, Ranking Member Schakowsky, and  
429 members of the Subcommittee, I am Jessica Rich, Director of  
430 the Bureau of Consumer Protection at the Federal Trade  
431 Commission. I appreciate the opportunity to present the  
432 Commission's testimony on the Subcommittee's data security  
433 legislation.

434 Reports of data breaches affecting millions of Americans  
435 fill the headlines. These breaches involved not just  
436 financial data, but other types of sensitive data, such as  
437 medical information, account credentials, and even the  
438 contents of private e-mails. These events serve as a  
439 constant reminder that consumers' data is at risk. Hackers  
440 and others seek to exploit vulnerabilities, obtain consumers'

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

441 sensitive information, and misuse it in ways that can cause  
442 serious harms to consumers and businesses. Indeed, identity  
443 theft continues to be the FTC's number one source of consumer  
444 complaints, and data shows that over 16 million consumers  
445 were victimized in 2012 alone.

446       Every year new incidents are reported that re-ignite  
447 concern about data security, as well as debate about the best  
448 way to provide it. Companies must implement strong data  
449 security measures to minimize consumers' risk of fraud,  
450 identity theft, and other substantial harm. Poor data  
451 security practices also creates risks for businesses. Data  
452 breaches can harm a company's financial interest and  
453 reputation, and also result in the loss of consumer trust.  
454 We need strong legislation now for consumers and the health  
455 of the commercial marketplace.

456       As the Nation's consumer protection agency, the FTC is  
457 committed to protecting consumer privacy and promoting data  
458 security in the public sector--private sector, excuse me.  
459 The FTC would like to thank the Subcommittee for proposing  
460 enactment of Federal data security and breach notification  
461 law, which the Commission has long supported on a bipartisan

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

462 basis.

463           The Commission supports a number of elements in the  
464 proposed legislation which will give us additional tools to  
465 deter unlawful conduct. First, the bill includes a provision  
466 requiring companies to implement reasonable data security  
467 standards in addition to breach notification, both of which  
468 are essential to protect consumers. Second, the legislation  
469 gives the FTC jurisdiction to bring cases against non-profits  
470 and common carriers. Third, the bill provides for civil  
471 penalties, which are important to ensure adequate deterrents.

472           However, other aspects of the draft legislation don't  
473 provide the strong protections needed to combat data  
474 breaches, identity theft, and other substantial consumer  
475 harms. First, the bill does not cover precise geolocation  
476 and health data, even though misuse of this and other  
477 information can cause real harm to consumers, and even though  
478 a lot of health information is not, in fact, covered by  
479 HIPAA. For example, we brought a case last year against a  
480 medical transcription company whose lax security practice  
481 resulted in psychiatrists' notes about individual patients  
482 being made available on the Internet, available through

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

483 simple Google searches. Given the definition of personal  
484 information in this bill, we would not be able to rely on the  
485 legislation to bring that case and seek civil penalties.

486 In addition to companies being careless with consumer  
487 information, hackers have incentives to obtain this data,  
488 even when it is not financial. For example, in some of our  
489 recent investigations, we have seen bad actors hack into  
490 company systems to steal consumers' information so they can  
491 extract payments from the companies for its return. A number  
492 of state laws currently protect consumers' health  
493 information, but those protections would be preempted under  
494 the bill.

495 Second, the Commission believes that data security  
496 protection should apply to devices that collect data, such as  
497 some Internet-enable devices. Breaches involving these  
498 devices raise broader safety concerns, even if no data is  
499 stolen. For example, if a pacemaker isn't properly secured,  
500 a breach could result in serious harm to the person using it.  
501 Similarly, a malicious criminal who hacks into a car's  
502 network could disable its brakes, and other safety features.

503 Third, the FTC continues to believe that data security

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

504 and breach legislation should include rulemaking authority  
505 under the Administrative Procedures Act. Rulemaking would  
506 allow the Commission to ensure that, as technology changes,  
507 and the risks from the use of certain types of information  
508 evolve, the law keeps pace, and consumers are adequately  
509 protected.

510 Finally, the FTC believes that any trigger for providing  
511 notification should be sufficiently balanced so that  
512 consumers can protect themselves when their data is at risk  
513 without experiencing over-notification. Accordingly, we  
514 support an approach that requires notice, unless a company  
515 can establish that there is no reasonable likelihood of  
516 economic, physical, or other substantial harm.

517 Thank you very much for this opportunity to provide the  
518 Commission's views. The FTC remains committed to promoting  
519 reasonable security for consumer data, and stands ready to  
520 work with the Subcommittee as it develops and considers  
521 legislation to protect consumers' sensitive information.

522 [The prepared statement of Ms. Rich follows:]

523 \*\*\*\*\* INSERT A \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

524           Mr. {Burgess.} The Chair thanks the gentlelady. Mr.  
525 Johnson, you are recognized for 5 minutes for the purpose of  
526 an opening statement.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

527 ^STATEMENT OF CLETE JOHNSON

528 } Mr. {Johnson.} Thank you very much. Dr. Burgess,  
529 Ranking Member Schakowsky, leaders of the full Committee,  
530 distinguished members, thank you very much for having--for  
531 providing the opportunity to discuss the FCC's current  
532 programs and authorities regarding consumer protections for  
533 communications data, privacy, security, and breach  
534 notification. For decades Congress has recognized that  
535 information related to consumers' use of communications  
536 services is especially sensitive for reasons that go beyond  
537 potential economic harm, such as financial fraud or identity  
538 theft. If Americans can't communicate privately, if we are  
539 not secure in the privacy of information about our  
540 communications, then we can't fully exercise the freedoms and  
541 rights of open democratic society. As with medical and  
542 health data--health care data, governed under HIPAA, and  
543 financial data, governed under Gramm-Leach-Bliley, and other  
544 statutes, Congress has long treated communications-related  
545 consumer information as a special category of consumer data



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

546 that calls for expert oversight, tailored protections, and  
547 specific enforcement.

548         Given recent developments, the privacy and security of  
549 sensitive information held by communications networks is  
550 actually a much bigger issue now than ever before. For  
551 example, public concerns about the availability of telephone  
552 call records, the widespread use of fixed and mobile  
553 broadband communications, privacy implications of crucial  
554 life-saving improvements to next generation 911, and finally,  
555 recent cyberattacks, such as the one aimed at suppressing the  
556 release and viewing of a motion picture. As the expert  
557 agency that regulates communications networks, we continually  
558 seek to improve these protections for the good of  
559 communications consumers. I will now turn to the legal  
560 framework currently in place to protect these communications  
561 consumers, and also the responsibilities of communications  
562 providers to secure their networks in the first place. The  
563 draft bill would alter this legal framework significantly,  
564 and would leave gaps, as compared to existing consumer  
565 protections for communications consumers.

566         First, Section 222 of the Act establishes a duty for

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

567 telecommunications carriers and interconnected VOIP providers  
568 to protect the confidentiality of consumers' proprietary  
569 information, including call records, location information,  
570 and other information related to the telephone service, such  
571 as the features of the customer's service, or even the  
572 customer's financial status. FCC rules under Section 222  
573 require carriers to notify law enforcement and consumers of  
574 breaches, and carriers that fail to meet these requirements  
575 are subject to an enforcement action.

576         Second, Sections 631 and 338(i) apply to cable and  
577 satellite TV providers, and they protect consumers' viewing  
578 history. That is the TV shows they watch, and the movies  
579 that they order, as well as any other personally identifiable  
580 information available to the service provider. Here too the-  
581 -these protections are enforced by FCC enforcement activity.  
582 And I would note that many of these protections, including  
583 those protections for several particular types of proprietary  
584 information, would no longer exist under the draft bill.

585         If enacted, Section 6(c) of the draft bill would declare  
586 sections of the Communications Act, as they pertain to data  
587 security and breach notification, to ``have no force or

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

588 effect'', except with regard to 911 calls. The Federal Trade  
589 Commission would be granted some, but not all, elements of  
590 the consumer protection authority that the FCC presently  
591 exercises. For example, if the draft bill were to become  
592 law, the FTC would not have the authority to develop rules to  
593 protect the security of consumers' data, or to update  
594 requirements as new security threats emerge, and technology  
595 evolves.

596       Finally, while the draft bill attempts to maintain the  
597 protections of the Communications Act for purposes other than  
598 data security, the FCC's experience implementing privacy and  
599 security requirements for communications consumer data shows  
600 that there is no simple distinction between these two  
601 interrelated concepts, privacy and security. Whether a  
602 company, number one, either by human or--human error or  
603 technical glitch, mistakenly fails to secure customer data,  
604 or, number two, if it deliberately divulges or uses  
605 information in ways that violated consumer privacy regarding  
606 that data, that--the transgression is at once a privacy  
607 violation and a security breach. In many cases it is the  
608 very same thing, and they--there--it is very difficult,

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

609 practically or legally, to separate the two.

610 I thank you again for the opportunity to provide a  
611 summary of the FCC's programs regarding data privacy and  
612 security, and, of course, look forward to answering any  
613 questions the Subcommittee may have. We at the FCC, of  
614 course, stand ready, and willing, and able to provide any  
615 input or assistance the Subcommittee may request as it  
616 completes this important work. Thank you very much.

617 [The prepared statement of Mr. Johnson follows:]

618 \*\*\*\*\* INSERT B \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

619           Mr. {Burgess.} Chair thanks both the witnesses for  
620 their forthright testimony. We will now go to the  
621 questioning portion of the hearing. I will recognize myself  
622 for 5 minutes for the purposes of questions.

623           Let me ask the same question to both of you. First, for  
624 the Federal Trade Commission, how many data security cases  
625 has the Federal Trade Commission brought to date? And, as a  
626 corollary, do you have an idea as to how many investigative  
627 hours have been spent on data security cases?

628           Ms. {Rich.} We have brought 55 data security cases,  
629 that is since the early 2000s, but we have actually brought  
630 hundreds of, combined, privacy and data security cases, held  
631 35 workshops, completed 50 reports. We have spent--I  
632 actually haven't tabulated up man hours, but it is an  
633 enormous amount, because for every case we bring, there are  
634 actually quite a number of investigations that we look into,  
635 but we decide not to bring a Federal court action. So it is  
636 millions of hours.

637           Mr. {Burgess.} Okay, but the total cases was 55, was  
638 your response?

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

639           Ms. {Rich.} In the data security area, but many of the  
640 privacy cases have some data security element too, and there  
641 are hundreds of those.

642           Mr. {Burgess.} Very well. Mr. Johnson, let me just ask  
643 the same question to you. How many data security cases has  
644 the Federal Communications Commission brought, and then,  
645 likewise, the investigative hours that you have--that your  
646 commission has spent on the data security cases?

647           Mr. {Johnson.} Thank you, Mr. Chairman. In the 18  
648 years that Section 222 has been in place, and this is the  
649 section that pertains to--primarily to telephone call  
650 records, there have been--I don't have the precise number,  
651 but I think it is in the realm of scores and scores of cases  
652 that pertain to what is called customer proprietary network  
653 information. This is call records, location information,  
654 time and duration of call, and a whole host of other what is  
655 called CPNI protections. I don't have the precise number,  
656 and I can certainly get you the precise number, nor the total  
657 accumulated hours, but it is scores and scores.

658           Mr. {Burgess.} To the extent--I think it would be  
659 helpful to the Subcommittee if you could make the actual

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

660 numbers available, and certainly--

661 Mr. {Johnson.} Of course.

662 Mr. {Burgess.} --I would allow you to do that for the  
663 record. Let me just ask you a question. You brought up the  
664 Consumer Proprietary Network Information. How many years  
665 after the 1996 Act did it take to fully implement the rules  
666 for CPNI at the Federal Communications Commission?

667 Mr. {Johnson.} Well, I think that that--I don't know  
668 the--which exact rule you are referring to, Mr. Chairman, but  
669 there--I think the broad answer is that it is a--it has been  
670 underway for 18 years, and there have been multiple  
671 improvements and shifts, including for Congressional  
672 expectation, technological development, for instance, voice  
673 over IP, location information Ms.--that is--pertains to 911.  
674 And in 2013 there was a declaratory ruling that the  
675 Commission declared that CPNI pertains to information that is  
676 collected on mobile devices.

677 So I guess the accurate answer is that it is--it remains  
678 a work in progress, and that is part of the value of having  
679 that rulemaking authority, is in order to adapt to  
680 Congressional expectations, changes of technology.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

681           Mr. {Burgess.} Maybe for the purposes of clarification  
682 for the Subcommittee, as we work through some of these  
683 issues, could the Commission provide us a timeline, from 1996  
684 to present, where the rulemaking was involved, where it  
685 evolved? Obviously the threat changed over that time as  
686 well. But I am--I guess, you know, that is part of my  
687 concern, is that it--I get the impression that it took some  
688 time from '96 to the point where the rulemaking had evolved  
689 to a point where there were actually consumer protections  
690 that were available. But I don't know that, and you are--

691           Mr. {Johnson.} Absolutely. I will take that--I think  
692 that is a very important homework assignment for me, and I--  
693 run through very briefly--the section was established in  
694 1996.

695           Mr. {Burgess.} Right.

696           Mr. {Johnson.} In 1999 location information was added.  
697 In 2007 there was a major problem with what is called pre-  
698 texters. And in my old world in--working on intelligence  
699 policy, this is essentially a human intelligence collector,  
700 where pre-texters would call the telephone company, ask--

701           Mr. {Burgess.} Right. We had a hearing on it here in



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

702 this Committee several years ago as well.

703           Mr. {Johnson.} And so that was something, again, that  
704 was at once a privacy and security issue, and in 2007 the  
705 Commission issued rules specific to solving that problem.  
706 And, again, there have been some other adjustments and  
707 improvements in recent years. But we will get you the full  
708 story. It is actually--it is--it is an important story about  
709 the development of Section 222.

710           Mr. {Burgess.} The Chair appreciates the gentleman's  
711 willingness to provide the information. The Chair recognizes  
712 Ms. Schakowsky. Five minutes for questions, please.

713           Ms. {Schakowsky.} I just want to clarify that my  
714 concerns between the agencies is really with regard to the  
715 impact on consumers. I don't want anything I say to seem to  
716 reflect a preference for one agency over another, but rather  
717 for the protection of the consumers.

718           So my--if this draft were enacted, regulatory and  
719 enforcement authority over data security and breach  
720 notification that is currently granted to the FCC would--  
721 under certain sections of the Communications Act and its  
722 regulations would have no force or effect. It is my

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

723 understanding that the data security and breach notification  
724 protections under the Communications Act are broader than the  
725 protections afforded under this draft. The Communications  
726 Act provides security protections for information regarding  
727 telecommunications subscribers' use of service, but this  
728 draft does not provide security protections for all of that  
729 information. Instead, it covers only ``the location of,  
730 number from which, and to which a call is placed, and the  
731 time and duration of such call''.

732         So, Mr. Johnson, what other information is currently  
733 protected under Title II of the Communications Act that would  
734 not be covered under this draft?

735         Mr. {Johnson.} Ma'am, you are correct it--that there  
736 are specific pieces of information, both under Section 222  
737 and also the cable/satellite provisions, that are not  
738 protected under this draft. With regard to Section 222,  
739 information such as how many calls a person has made, you  
740 know, sort of the peak calling periods for that person, does  
741 this person make phone calls in the morning, at night,  
742 lunchtime, specific features of the service, like call  
743 waiting, caller ID, and then other things that may be

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

744 pertinent to call service, like this--like the financial  
745 status of the customer. Is the customer--does the customer  
746 qualify for Medicaid, or SNAP, or other low income support?  
747 Those would explicitly not be protected by the definition in  
748 the draft bill.

749 On the cable and satellite side, it is--essentially all  
750 of it would not be protected. What television shows you  
751 watch on cable and satellite, what pay-per-view you order,  
752 what you order from the Home Shopping Network, none of this  
753 would be protected under the draft bill, and it is--

754 Ms. {Schakowsky.} So--

755 Mr. {Johnson.} --presently protected.

756 Ms. {Schakowsky.} So viewing preferences, or viewing  
757 history, none of that would be covered?

758 Mr. {Johnson.} It is presently covered. It would not  
759 be covered under the draft bill.

760 Ms. {Schakowsky.} No, that is what I am talking about.  
761 This bill also voids breach notification obligations required  
762 under the Communications Act, Mr. Johnson, and its  
763 regulations, but as I read it, the bill would not require  
764 breach notification for a breach of call information. Under

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

765 the Communications Act, and associated regulations, a breach  
766 of customer information, such as call data and viewing  
767 habits, requires notice to law enforcement and affected  
768 customers. Is that right?

769 Mr. {Johnson.} That is correct.

770 Ms. {Schakowsky.} But as we established, much of the  
771 customer information currently required to be secured under  
772 the Communications Act does not have to be secured under this  
773 bill. And if there is no requirement to protect the  
774 information, then there is no requirement to provide notice  
775 in the event of a breach, correct?

776 Mr. {Johnson.} That is correct.

777 Ms. {Schakowsky.} And even for the limited call  
778 information that must be secured under this bill, a breached  
779 company would not be required to provide notice because call  
780 information is not financial in nature, do you agree?

781 Mr. {Johnson.} That is my interpretation, yes, ma'am.

782 Ms. {Schakowsky.} So I wondered, Ms. Rich, if you  
783 wanted to comment on that. This is a concern that I have for  
784 consumers, that I think if we allowed the FCC to continue in  
785 its regulations, that we could then make sure we cover

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

786 everything.

787 Ms. {Rich.} We--for consumers--we are also looking at  
788 this bill in terms of its effect on consumers, and that is  
789 why, in our testimony, we have proposed that the bill apply  
790 to more information, geo, health. Communications would also  
791 be something that should be added to the bill. We also  
792 believe the breach notification trigger should be a bit  
793 broader to encompass different harms. So that, we agree,  
794 would be an improvement to the bill.

795 But I--as to jurisdiction, I should say that our  
796 position is that we should have jurisdiction in this bill.  
797 The FTC should have jurisdiction over carriers in this bill  
798 because we have brought so many cases in this area. We bring  
799 so much enforcement expertise to the table. We really have  
800 been working on this issue since, really, the mid '90s. We  
801 also believe we should be able to hold different companies  
802 that are collecting some of the very same type of information  
803 to the same standards on--in our enforcement. You know,  
804 Netflix, Google, and Verizon really have a lot of the same  
805 information.

806 And, further, the--we haven't taken a position on

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

807 reclassification, but one byproduct of reclassification is it  
808 does remove our FTC jurisdiction from over providers of  
809 broadband service, so we would actually be--we are actually  
810 able to do less post-reclassification to help consumers than  
811 we were able to do before. That being said, we believe--a  
812 majority at the Commission believes we should share  
813 jurisdiction with the FCC, and not displace the FCC.

814 Ms. {Schakowsky.} Thank you. I yield back.

815 Ms. {Rich.} We work very well together.

816 Ms. {Schakowsky.} Thank you.

817 Mr. {Burgess.} Gentlelady's time has expired. The  
818 Chair recognizes the gentleman from Michigan, the Chairman of  
819 the full Committee, Mr. Upton. Did he--about--Ms. Blackburn,  
820 then, you are recognized to have 5 minutes for questions,  
821 please.

822 Mrs. {Blackburn.} Thank you, Mr. Chairman, and I want  
823 to thank our witnesses for being here.

824 Mr. Johnson, to you first. Please get your facts and  
825 figures all in order, as Chairman Burgess asked, and get that  
826 back to us. It is helpful--

827 Mr. {Johnson.} Yes.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

828           Mrs. {Blackburn.} --to us, and we were hopeful to have  
829 that information today to be able to define the number of  
830 data security cases that you all have brought forward, not  
831 just terming it scores and scores. So let us tighten that up  
832 for the record.

833           Ms. Rich, to you, you talked about the 55 cases that you  
834 all have brought forward, so I want you to walk me through  
835 what is the criteria that you utilize when you decide to  
836 bring a case forward? What is--what goes into that decision  
837 matrix?

838           Ms. {Rich.} The core concept in our data security  
839 program, whether--and we have several different laws we  
840 enforce, is reasonableness, and not whether there has been a  
841 breach. And we have emphasized a process-based approach that  
842 is tech neutral. So for years we--our education and our  
843 cases have been emphasizing that the key to data security is  
844 to put--is to follow certain key, you know, basic common  
845 elements, put somebody in charge, make somebody responsible  
846 for the program, do a risk assessment to determine what are  
847 the risks in your business, not some checklist that another  
848 business with a totally different business model is using,

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

849 develop a program to address the risks you have just found,  
850 and focus in particular on things like the key area--

851 Mrs. {Blackburn.} Let me interrupt you there.

852 Ms. {Rich.} Yeah.

853 Mrs. {Blackburn.} Would you consider, then, that this  
854 is more along--you all have an informal set of best practices  
855 that you refer back to? Would that be a fair statement?

856 Ms. {Rich.} Yeah. It is not really informal, because  
857 it has been widely publicized in the education materials we  
858 put out in our complaints and orders, which all re-iterate  
859 these same elements.

860 Mrs. {Blackburn.} Okay. All right. Let me ask you  
861 this, then. Do you think the draft legislation would limit  
862 the FTC's Section 5 authority?

863 Ms. {Rich.} Well, there is a savings clause, and we are  
864 happy about that, but, you know, as we understand it, this is  
865 a discussion draft, and so right now we have some concerns  
866 that it might weaken the protections that are currently in  
867 place. But with the--some of the suggestions we have made  
868 for strengthening the bill, we believe it could be quite  
869 strong.



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

870 Mrs. {Blackburn.} Okay. So you would rather--okay, let  
871 me ask you about this, then. What about consent orders? You  
872 all have to go ahead and get that consent order to obtain  
873 civil penalties for unfair or deceptive practices, so do you  
874 believe consent orders are a strong incentive for industry  
875 for instituting data security civil penalties?

876 Ms. {Rich.} We--you are making an excellent point,  
877 which is that the bill's inclusion of civil penalties is  
878 critical, and we are very supportive of that. Right now, as  
879 you note, in order for us to obtain civil penalties, which  
880 believe are an important incentive and deterrent from bad  
881 behavior, we have to obtain an administrative order first,  
882 and then, if there is a violation, obtain civil penalties.  
883 So yes, you are absolutely right, that civil penalties are a  
884 key ingredient to the success of legislation.

885 Mrs. {Blackburn.} Okay. With that, I am going to yield  
886 back my time, Mr. Chairman, so we can move on with the rest  
887 of the questions.

888 Mr. {Burgess.} Appreciate--the gentlelady yields back.  
889 Chair recognize the gentleman from Massachusetts, Mr.  
890 Kennedy, 5 minutes for questions, please.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

891           Mr. {Kennedy.} Thank you, Mr. Chairman. And, again,  
892 thank you to the witnesses for testifying. I appreciate the  
893 information that you have already offered us today, and as we  
894 go through this process.

895           The FCC has enacted strong regulations to implement  
896 their authorities under the Communications Act, and I know  
897 you have touched on that a little bit already. These  
898 regulations require telecommunications providers to implement  
899 a number of specific privacy and security measures to protect  
900 consumer proprietary information. I wanted to walk through,  
901 with both of you, a little bit about some of those  
902 requirements so we can flesh this out a little bit.

903           So, Mr. Johnson, these regulations require that  
904 telecommunications carriers take steps not only to secure  
905 customer information, but also discover attempts to gain  
906 unauthorized access to that information, isn't that right?

907           Mr. {Johnson.} That is correct.

908           Mr. {Kennedy.} So carriers also, then, must  
909 authenticate a customer before providing customer information  
910 over the phone, online, or in a store as well?

911           Mr. {Johnson.} That is correct.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

912           Mr. {Kennedy.} Carriers are required to train their  
913 employees in the use of that customer information, is that  
914 right?

915           Mr. {Johnson.} That is correct.

916           Mr. {Kennedy.} Okay. Are there some other things that  
917 are required under the FCC's regulations that you would like  
918 to highlight as well?

919           Mr. {Johnson.} In addition to the--to those that you  
920 laid out, Congressman, also--carriers are also required to  
921 discipline abuses and to certify compliance with these rules.  
922 And, if I may, I would add to that the distinction between  
923 enforcement and rulemaking clarity. Of course enforcement is  
924 a crucial part of compliance, and the FCC has an Enforcement  
925 Bureau that is very active in this space, as is the FTC in  
926 the--we partner together on--in many areas, and expect to in  
927 the future as well.

928           The distinction between the present protections in 222  
929 and an enforcement only approach is that the FCC, or in that--  
930 -in this case, the FTC, if this bill were to be enacted, the  
931 FCC presently has the ability to get out and engage the  
932 public, the providers, to work together through advisory

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

933 committees, through rulemaking processes, through a whole  
934 host of measures, to make clear what the challenges are and  
935 what the solutions are before there is a problem. So instead  
936 of post hoc enforcement only, there is a solving the problem  
937 before it happens, or once it has been spotted, in the case  
938 of pre-texting, Mr. Chairman, that you can go after this  
939 problem, and seek to solve it, instead of just post hoc--

940 Mr. {Kennedy.} So proactive versus reactive, right?

941 Mr. {Johnson.} That is right.

942 Mr. {Kennedy.} And--so would those requirements be  
943 preempted under the current legislation?

944 Mr. {Johnson.} They would be eliminated.

945 Mr. {Kennedy.} So, Ms. Rich--thank you, Mr. Johnson.  
946 Ms. Rich, if, for example, a telecommunications provider  
947 disclosed the number of calls that I made from a specific  
948 phone number to a third party, would the FTC be able to bring  
949 an enforcement action under this bill?

950 Ms. {Rich.} We believe that should be added to the  
951 bill.

952 Mr. {Kennedy.} Okay. And would the FTC be able to  
953 require that telecommunications providers not disclose that

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

954 information unless they obtain customer consent, or should  
955 that be added as well?

956 Ms. {Rich.} Well, that would be a privacy provision, so  
957 I am not sure it would be addressed by this bill. But--and I  
958 don't think that would be preempted by this bill, the privacy  
959 provisions of the CPNI rules. But, in any event, we do think  
960 communications should be added to the bill as an element--a  
961 data--a piece of data that should be covered.

962 Mr. {Kennedy.} Okay. I appreciate the feedback. Thank  
963 you very much, and I yield back.

964 Mr. {Burgess.} Gentleman yields back. The Chair now  
965 will recognize the Vice Chair of the Subcommittee, Mr. Lance.  
966 5 minutes for questions, please.

967 Mr. {Lance.} Thank you, Mr. Chairman. Good morning to  
968 you both.

969 To Ms. Rich, the FTC has been a strong advocate for  
970 protection of Social Security Numbers, and has often  
971 indicated that Social Security Numbers are closely tied to  
972 identity theft. I don't think there is any doubt about that.  
973 How many state data security and breach notification bills  
974 include Social Security Numbers alone as personal

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

975 information?

976 Ms. {Rich.} We have that information, but I don't have  
977 it at my fingertips, but we would be happy to provide it to  
978 the Committee.

979 Mr. {Lance.} Thank you very much. Mr. Johnson, did you  
980 have an opinion on that?

981 Mr. {Johnson.} I don't know the answer to that--

982 Mr. {Lance.} Certainly. Thank you. To Ms. Rich, do  
983 you support the inclusion of standalone Social Security  
984 Numbers as personal information in the draft legislation?

985 Ms. {Rich.} Yes. We were very happy to see that in the  
986 bill.

987 Mr. {Lance.} Thank you. And are these data elements  
988 not listed in the draft legislation that the FTC has seen  
989 tied to identity theft and payment fraud? Are there any data  
990 elements not listed in the draft legislation that you would  
991 like to see in it?

992 Ms. {Rich.} Yes. In addition to Social Security  
993 Number, driver's license and passport number, and other  
994 government issued numbers can also be used to perpetrate  
995 identity theft, so we would like to see that information

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

996 protected standalone, and now it needs to be coupled with  
997 other information.

998           We have also believed that medical--that health  
999 insurance numbers can lead to medical identity theft, where  
1000 people charge--place charges on--in hospitals billed to other  
1001 people, and it can really accumulate, and they can do that  
1002 with simply health insurance numbers. And I believe those  
1003 are the main elements, besides health and geolocation, which  
1004 we are not talking about identity theft, we are talking about  
1005 other information that should be protected. But those are  
1006 the main additional elements.

1007           Mr. {Lance.} So, to reiterate, other than Social  
1008 Security, driver's license, and then health identification  
1009 numbers?

1010           Ms. {Rich.} Yes.

1011           Mr. {Lance.} Thank you. Mr. Chairman, I yield back the  
1012 balance of my time.

1013           Mr. {Burgess.} Chair thanks the gentleman, the  
1014 gentleman yields back. The Chair recognizes the gentleman  
1015 from Vermont, Mr. Welch. Five minutes for questions, please.

1016           Mr. {Welch.} Thank you very much. And I thank the

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1017 witnesses for your very helpful testimony. Just by way of  
1018 introduction, I think we have got some areas of real  
1019 agreement here. Number one, bipartisan agreement that this  
1020 is a brutal problem. Number two, it is the Wild West. There  
1021 is no clarity about who is in charge, or what the enforcement  
1022 is. Number three, there is a desire to get things done that  
1023 are going to add protection, rather than take it away.

1024       There is some disagreement on policy matters. Like, for  
1025 instance, on--you, Ms. Rich, indicated you want a stronger--  
1026 or as you call it, a stronger trigger notice, and where that  
1027 balance is--you used that word, balance, that is a debatable  
1028 proposition. You know, I happen to think that the notice  
1029 provisions under Gramm-Leach-Bliley--I don't know if you have  
1030 refinanced your mortgage at all, but you get so much  
1031 information it is useless, so I want to balance where  
1032 consumers are protected and notified, but not terrified, and  
1033 that is a discussion in a debate.

1034       But there are other areas where--for instance, with Ms.  
1035 Schakowsky, she raised what I thought were some really valid  
1036 concerns, and this is with respect to the transition of  
1037 authority. Because my view of the language is that the CPNI



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1038 that would go to the FTC, you would have that enforcement  
1039 authority. And the bottom line for me is the concern, which  
1040 I think is what Ms. Schakowsky was expressing, do we protect  
1041 the consumers, as opposed to who is in charge.

1042 And I actually do share that, but the privacy provisions  
1043 that you were talking about, Mr. Johnson, my understanding,  
1044 and I think, Ms. Rich, you testified to this, the privacy  
1045 provisions that FCC has would be retained, and not preempted,  
1046 correct? That is your view, Ms. Rich?

1047 Ms. {Rich.} I would defer to my colleague on that.

1048 Mr. {Welch.} No, I want to ask you, because if we have,  
1049 essentially, a situation where we think we are in agreement,  
1050 but we have language that we are uncertain meets the  
1051 agreement that we think we have, then that is a different--  
1052 the nature of that is a different challenge. It is like  
1053 trying to get the language right. And I appreciate Ms.  
1054 Blackburn and Mr. Burgess for focusing on, you know, trying  
1055 to define what the problem is, rather than create additional  
1056 problems. But my understanding of your testimony was that  
1057 you believe that privacy was not preempted, correct?

1058 Ms. {Rich.} If I have the current version of the

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1059 legislation, I thought I saw in there that the privacy  
1060 provisions of the CPNI rules, and other portions of the  
1061 Communications Act, were retained.

1062 Mr. {Welch.} Right. And, Mr. Johnson, is that your  
1063 view as well?

1064 Mr. {Johnson.} Yes, sir. I do think that that is--the  
1065 language attempts to divide privacy from security.

1066 Mr. {Welch.} All right. So let us say we got the  
1067 language right to your satisfaction, and the FTC took over  
1068 authority for CPNI, and you retained--the FCC retained the  
1069 current jurisdiction it has for privacy. From an agency  
1070 standpoint, that might not be your preference, but from a  
1071 consumer standpoint, you would still be holding folks  
1072 harmless with a new enforcer on some of the elements, is that  
1073 right?

1074 Mr. {Johnson.} Sir, I would actually say that it is not  
1075 possible to divide privacy from security, because in most  
1076 cases the security of information is the privacy of the  
1077 information, and vice versa. So, for instance, if you have  
1078 an insider threat, if there is a bad actor in your company,  
1079 or a mistaken actor in your company, and that person has

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1080 authorized access to the information, but then mishandles it,  
1081 or commits some sort of--

1082 Mr. {Welch.} Okay, I am--I appreciate that, and I am  
1083 going to ask you to help us here, because the spirit that our  
1084 Chairman has provided here I think is really good. The big  
1085 problem for everyday people in Vermont is their financial  
1086 information. A lot of these other things that you have  
1087 mentioned, they are important, and we have got a lot of work  
1088 in this Congress to deal with privacy questions--

1089 Mr. {Johnson.} Um-hum.

1090 Mr. {Welch.} --but the--90 percent of the problem for  
1091 100 percent of the people is loss of their identity and their  
1092 financial information. And, you know, the bad guys out  
1093 there, that is what they want.

1094 Mr. {Johnson.} Um-hum.

1095 Mr. {Welch.} If they want my Social Security Number, it  
1096 is not for any reason other than to get to my bank account.

1097 Mr. {Johnson.} Right.

1098 Mr. {Welch.} So I think the focus here of a narrow  
1099 approach that Mr. Burgess has adopted, I think, makes some  
1100 sense. Now, if there--we don't want to lose rights that

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1101 people have, but we may need the help of the FTC and the FCC  
1102 to write that language so that we accomplish this goal that  
1103 we are accepting is narrow, but without compromising other  
1104 rights.

1105 Mr. {Johnson.} I--

1106 Mr. {Welch.} So--

1107 Mr. {Johnson.} And I--if I may, sir, I, of course,  
1108 commend you, and all of you, for trying to tackle this issue.  
1109 When I was a Senate staffer on the other side, I tried it as  
1110 well, and we didn't quite get there. It is--I think there--  
1111 the two things with regard to consumer protections that I  
1112 would like to mention are, number one, with regard to  
1113 communications consumer protections, it is a different type  
1114 of information.

1115 And I think you will hear in this next panel some very  
1116 expert, knowledgeable witnesses say that data is data, a  
1117 server is a server, and I would just respectfully disagree  
1118 that, with regard to call data, with regard to data that  
1119 flows over networks, cable/satellite, it is specific to the  
1120 network engineering, and how these networks actually--

1121 Mr. {Welch.} All right. My time is running out, but

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1122 here is the one request I am going to make of you. You have  
1123 identified a problem. We need you to identify a solution,  
1124 because this is not a policy difference that you are  
1125 describing now. This is a practical challenge that you are  
1126 describing. Let us get your help in solving that.

1127 Mr. {Johnson.} --absolutely.

1128 Mr. {Welch.} I yield back.

1129 Mr. {Burgess.} Chair thanks the gentleman. Gentleman's  
1130 time has expired. The Chair recognizes the gentleman from  
1131 Texas, Mr. Olson. Five minutes for questions, please.

1132 Mr. {Olson.} I thank the Chair. Welcome, Mrs. Rich,  
1133 and Mr. Johnson. Sadly, data breaches have become common  
1134 news. Just this morning we learned about Primera Health  
1135 Care. 12 million of their customers lost their data, had it  
1136 exposed to hackers. They were attacked in May, discovered  
1137 the attack in January, and found out recently what had  
1138 happened. We can do better, but we need to take a balance  
1139 approach to data breach notifications. We have to protect  
1140 consumers, but we can't be a burden to companies and hinder  
1141 the legal uses of data.

1142 This draft doesn't fix all the problems, but it is a

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1143 small but important step in the right direction. I have a  
1144 few questions for you this morning. The first ones are for  
1145 you, Ms. Rich. How many people work in your division in the  
1146 FTC?

1147 Ms. {Rich.} We have a privacy division of about 45  
1148 people, but we have a number of regional offices, and a  
1149 number of other offices that work on various privacy issues,  
1150 like Do Not Call, or privacy issues related to financial  
1151 information, so we have quite a number of people working on  
1152 privacy. We, of course, could always use more, but--yeah.

1153 Mr. {Olson.} How many folks on data security? All 45,  
1154 or more than 45? And how many people focus on data security  
1155 within the FTC, or your division?

1156 Ms. {Rich.} I don't have at my fingertips exactly, but  
1157 almost everyone in the division works on both privacy and  
1158 data security. And then, as I said, there are people in  
1159 other parts of the agency who also work on these issues. So--  
1160 -I can get you more information, if you would--

1161 Mr. {Olson.} Thank you.

1162 Ms. {Rich.} --like, but--yeah.

1163 Mr. {Olson.} Do they determine what a reasonable data

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1164 security practice is? Do they do that, as a matter of  
1165 policy?

1166 Ms. {Rich.} We have standards that we have put out,  
1167 both in our original Gramm-Leach-Bliley safeguards rule, in  
1168 all of our complaints and orders. As I said, we lay out a  
1169 process that is reasonable security. We consider, you know,  
1170 various factors, like the sensitivity and volume of data, et  
1171 cetera, and the staff attorneys who work on this follow the  
1172 standards that we follow throughout the agency, and that we  
1173 have announced to the public in particular cases.

1174 Mr. {Olson.} Do they make sure companies use good  
1175 practices? If so, how do they do that, ma'am?

1176 Ms. {Rich.} We--in investigations, we evaluate whether  
1177 reasonable security was followed, and whether these types of  
1178 processes I talked about was--were followed.

1179 Mr. {Olson.} And I am sure you have to have people with  
1180 very special skills. How hard is it to find those people?  
1181 Is that a problem for you, ma'am, need more people with the  
1182 skills to go after these hackers?

1183 Ms. {Rich.} We have very well trained attorneys and  
1184 investigators. We also have a lab unit that helps with--if

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1185 there is any forensics involved. And we have experts and  
1186 technologists, both on staff, and that we consult with.

1187 Mr. {Olson.} Thank you, Ms. Rich. Mr. Johnson, for  
1188 you, my friend, how many folks in your department work on  
1189 data security? Not cybersecurity, but data security, within  
1190 the FCC?

1191 Mr. {Johnson.} It--Congressman, I can get you a  
1192 specific answer. It is a little--ours--our--it is not  
1193 divided quite as neatly for us as it is at the FTC, in the  
1194 Consumer--

1195 Mr. {Olson.} Ballpark, 10, 20, 30?

1196 Mr. {Johnson.} I would say dozens of people work on  
1197 various aspects of this in the Public Safety Bureau, that is  
1198 the bureau that I am in, in the Enforcement Bureau, also the  
1199 Wireless Bureau, the Wire Line Bureau, the Media Bureau. It  
1200 is an issue that covers--in the Consumer Protection Bureau,  
1201 essentially every bureau of the FCC has a role in this in  
1202 some form or fashion.

1203 Mr. {Olson.} And how about finding really qualified  
1204 people? Hard time finding the people and skills you need at  
1205 the FCC to do your job with these data breaches?



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1206           Mr. {Johnson.} I would say that the FCC is--has the  
1207 most qualified network engineers and communications lawyers,  
1208 and, importantly, communications economists that I have run  
1209 across. It is an expert agency in the communications field.

1210           Mr. {Olson.} So it sounds like you balanced enforcement  
1211 with the market, communications, economics, and so you are  
1212 actually a partner in this endeavor, so thank you for that.  
1213 I am out of my time. Yield back.

1214           Mr. {Burgess.} The Chair thanks the gentleman. The  
1215 Chair now recognizes the gentleman from Illinois, former  
1216 Chairman of the Subcommittee, Mr. Rush. Five minutes for  
1217 questions, please.

1218           Mr. {Rush.} Thank you, Mr. Chairman. I really am  
1219 enjoying the input, and the conversation both ways, in  
1220 regards to this particular matter. I view the issue before  
1221 us as an issue that is really--that we have to maintain the  
1222 understanding that data security and privacy are really like  
1223 two sides of the same coin, and we can't bifurcate these two  
1224 issues.

1225           I think we have to proceed with, really, the  
1226 understanding that, in order to be forced to really serve the

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1227 American people, and begin to deal with this issues--these  
1228 issues that they are confronted with, both in terms of  
1229 privacy and also data security, that we can't waste our time  
1230 in trying to separate these two issues. And I don't think  
1231 the outcome would be an outcome that we want to achieve, and  
1232 that would really help us out in the problem that all of us  
1233 are vitally concerned about.

1234 I want to ask Ms. Rich, recently the FC announced that  
1235 broadband providers would be regulated as common carriers.  
1236 Under these particular rules, if a broadband provider were to  
1237 be the subject of a data breach, which agency would have  
1238 primary responsibility for ensuring that any Federal standard  
1239 is enforced? And, Mr. Johnson and Ms. Rich, I want you to  
1240 answer those question--this question, beginning with you, Ms.  
1241 Rich.

1242 Ms. {Rich.} Prior--we have not taken a position on  
1243 reclassification generally, but, as I mentioned, a byproduct  
1244 of it is we--it limits our ability to protect consumers when  
1245 the companies that perpetrate the violations are broadband  
1246 providers. So if a broadband provider had a breach, and it  
1247 was--pertained to their provision of broadband service, and

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1248 not some ancillary service, we would no longer be able to  
1249 protect service in that area. We would like, of course, to  
1250 have somebody, maybe somebody here, restore that jurisdiction  
1251 to us. We don't, however, object to the reclassification.

1252 Mr. {Rush.} Mr. Johnson, what are your--

1253 Mr. {Johnson.} Congressman--

1254 Mr. {Rush.} --comments?

1255 Mr. {Johnson.} We are--my focus in work, and also at  
1256 this hearing, is the--is--are the provisions that pertain to  
1257 data security of communications data. I am certainly aware  
1258 of the effect that Title II reclassification has,  
1259 particularly on Sections 201, 202, and 222. And I will just--  
1260 -if it is okay with you, I will leave it at that, because I  
1261 have never practiced law with regard to the Federal Trade  
1262 Commission Act, and I will defer to the Federal Trade  
1263 Commission, and--

1264 Mr. {Rush.} Well--okay. Well, thank you so much. Ms.  
1265 Rich, can you clarify one piece of your testimony, if you  
1266 will? You are advocating to lift the common carrier  
1267 exemption, but not to take away regulatory or enforcement  
1268 authority from the FCC, am I correct? That is--how would

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1269 that be done? What do you suggest?

1270 Ms. {Rich.} Well, we share jurisdiction with a lot of  
1271 different agencies in a lot of different areas, and, you  
1272 know, we have--for example, with the CFPB, we have an MOU  
1273 with them. We have, for years, shared jurisdiction with the  
1274 FCC as to do not call. We did share jurisdiction over  
1275 broadband providers, proprietor re-classification, and we can  
1276 successfully coordinate, and make sure there is no  
1277 duplication.

1278 So what we are saying is we think, as the agency that is  
1279 most experienced in the data security area has can be very  
1280 effective in protecting consumers that we should be--we  
1281 should have jurisdiction over carriers, but that we--that the  
1282 FCC--the majority of our commission believes that that  
1283 doesn't mean the FCC shouldn't--should be displaced in its  
1284 jurisdiction.

1285 Mr. {Rush.} Okay. Is there--in terms of the--your  
1286 practice that you have regarding these memorandum of  
1287 understandings, does that create a burdensome issue for the  
1288 consumer? Is there--does that complicate their lives, or--

1289 Ms. {Rich.} No, not for the consumer at all. In fact,

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1290 the consumer potentially has two cops on the beat. But what  
1291 the MOUs and the coordination is usually for is to make sure  
1292 that there is no duplication and burdens created for  
1293 businesses. For example, the two agencies, without  
1294 communicating with each other, both investigating the same  
1295 company at the same time.

1296 Mr. {Rush.} Mr. Johnson, you want to comment on--

1297 Mr. {Johnson.} I think she stated it very well, sir.

1298 Mr. {Rush.} Mr. Chairman, thank you, and I yield back.

1299 Mr. {Burgess.} Chair thanks the gentleman, the  
1300 gentleman yields back. The Chair recognizes the gentleman  
1301 from Kansas, Mr. Pompeo. Five minutes for questions, please.

1302 Mr. {Pompeo.} Thank you, Mr. Chairman, and thank you  
1303 both for being here today. I suppose I am not surprised, but  
1304 I am troubled by how little conversation there has been this  
1305 morning about cost to consumers. When you talk about  
1306 protecting consumers, there is very little discussion about  
1307 what this will mean, right? If a business is paying money,  
1308 it gets passed along, and there is just remarkably little  
1309 discussion about what it really means to someone who can  
1310 least afforded whatever services that we are dealing with. I

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1311 think that is very important.

1312 I would hope that the two of you would appreciate that  
1313 too, but instead what I get is two government agencies, each  
1314 of which wants increased authority, increased power, more  
1315 control, the capacity to define rights, sort of the historic  
1316 governmental actions. I would hope, when you think about the  
1317 consumers that you are tasked to oversee that you would at  
1318 least consider their economic well-being as well.

1319 Ms. Rich, in that vein, you have asked for a--you said  
1320 that the definition contained--really, the notice provision,  
1321 you weren't happy with it. You suggested alternative  
1322 language. You said you would support an approach that  
1323 ``requires notice, unless a company can establish there is no  
1324 reasonable likelihood of economic, physical, or other  
1325 substantial harm''. So you have flipped the burden of proof  
1326 now to the consumer, right? Right, to the business which  
1327 they have contracted with to demonstrate that there is no  
1328 harm. What do you think the cost of a change like that would  
1329 be?

1330 Ms. {Rich.} I think the burden is already flipped in  
1331 the draft. All we are proposing is that the--instead of it

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1332 being limited to financial harm, that it be--include  
1333 economic, physical, or other substantial harm.

1334 Mr. {Pompeo.} Fair enough. I want to go on to Mr.  
1335 Johnson. Mr. Johnson, you--I think in response to a question  
1336 you said that there were--you didn't know the exact date, or  
1337 you were going to bring us that, but you said there were  
1338 scores of cases? Is that right?

1339 Mr. {Johnson.} Yes, sir, of--

1340 Mr. {Pompeo.} That you brought? And you identified two  
1341 in your written testimony, if I got it right. Is--

1342 Mr. {Johnson.} I think the--if I remember correctly,  
1343 the two that are in the footnote in the written testimony--

1344 Mr. {Pompeo.} Right.

1345 Mr. {Johnson.} --were from--were just two examples from  
1346 last year that were concluded. I--we are--I would draw a  
1347 distinction between cases that are investigated, cases that  
1348 are pursued, cases that are settled, and not necessarily  
1349 cases that all end in a--

1350 Mr. {Pompeo.} Are these the only that have--that are of  
1351 record? You said there are scores and scores. There are two  
1352 identified. Are there others that you could have put in

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1353 this--

1354 Mr. {Johnson.} Absolutely. Yes, sir, and I committed  
1355 earlier--

1356 Mr. {Pompeo.} And would any of those have actually been  
1357 data breaches? Because neither of these, as described in  
1358 your testimony, are actually what we are dealing with here  
1359 today.

1360 Mr. {Johnson.} Well, I think the--

1361 Mr. {Pompeo.} One is a Do Not Call case, according to  
1362 your testimony, and one was a violation of--

1363 Mr. {Johnson.} That--yes, sir, that--your question  
1364 underscores the distinction that we think is important with  
1365 regard to communications data. It is not just breach of  
1366 Social Security Numbers or credit card numbers. It is about--  
1367 -information about what people do on the telephone, what do  
1368 they do with cable and satellite TV, and it is a much broader  
1369 set of data that is specific to the networks that hold, and  
1370 manage, and deliver that data.

1371 So it is not--it is harder for us to hone in on, this  
1372 was a data breach of Social Security Numbers, than it is to  
1373 talk about how we prospectively and proactively protect the



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1374 consumer in a way that is actually, I think, to your original  
1375 point, is cost effective, because it allows us to engage  
1376 ahead of time with the providers. And I can give a number of  
1377 examples about how we do that in a way that aligns it with  
1378 business interests to protect the consumer, while also  
1379 letting the companies sort of--

1380 Mr. {Pompeo.} Yeah.

1381 Mr. {Johnson.} --lead the solutions, yeah.

1382 Mr. {Pompeo.} I am not sure I agree with you. I went  
1383 back and read the Notice of Apparent Liability that you have  
1384 issued, and when you--the language you used implies that if  
1385 you have a breach, then your security is, per se,  
1386 unreasonable, and your privacy policy is deceptive. Is that  
1387 the FCC's position?

1388 Mr. {Johnson.} I don't know the exact line that you are  
1389 going at there, but if you are--do you know which action you  
1390 are referring to, sir?

1391 Mr. {Pompeo.} I do, but I just want to--I want to go  
1392 more generically. I want to kick it out from the particular  
1393 case. Is it the case that it is the FCC's view that it is a  
1394 per se--is, per se, unreasonable, and your privacy policy is

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1395 deceptive, if there was a breach?

1396 Mr. {Johnson.} No, sir, I don't think that is the case.

1397 In fact, in our rules, it requires--on the 222 side, it

1398 requires reasonable measures to discover and protect against

1399 unauthorized access.

1400 Mr. {Pompeo.} Great. Thank you. Mr. Chairman, my time

1401 is up. I yield back.

1402 Mr. {Johnson.} I should--do you--if I might, sir, the

1403 one additional note is that on the cable/satellite side, and

1404 this is another distinction with the bill, the standard is

1405 not just reasonable. It is as necessary to protect, so it is

1406 a much higher standard in the cable/satellite viewing

1407 preferences case.

1408 Mr. {Pompeo.} Thank you.

1409 Mr. {Johnson.} But it still--I wouldn't say it is a per

1410 se violation.

1411 Mr. {Burgess.} Chair thanks the gentleman. Gentleman's

1412 time has expired. The Chair recognizes Mr. Cardenas. Five

1413 minutes for questions, please.

1414 Mr. {Cardenas.} Thank you very much, Mr. Chairman. I

1415 want to thank the witnesses for all of your service. It is

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1416 an issue that is becoming more and more important. But one  
1417 thing that I would like to underscore is that I look at this  
1418 as similar to what we all, as Americans, thankfully, take for  
1419 granted, that in any community we have government police.  
1420 And let me tell you, when communities hire private policing,  
1421 or what have you, talk about things getting out of control,  
1422 and talk about lowering the standard of the kind of security  
1423 that community has.

1424         There is certainly a drastic difference between hiring a  
1425 security guard versus calling 911 and having the true police  
1426 force show up. So I want to thank both of you, and both of  
1427 your departments, for what you do for us to keep us safe.  
1428 And certainly to keep the cost effectiveness of your purpose  
1429 I believe is about American consumers, and making sure that  
1430 we fortify you with the resources you need so you can have  
1431 the intelligent individuals, and the hardworking individuals  
1432 to go ahead and make sure that breaches don't happen as often  
1433 as possible, we can be preventative.

1434         Because let me tell you, what we pay in taxes is nothing  
1435 compared to the person who gets their information breached.  
1436 They lose their house, their entire credit report goes to the

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1437 wastebasket, and they lose everything. And then in many,  
1438 many cases it is years, and years, and years before that  
1439 individual, or that family, can actually get back to being  
1440 right, and their entire reputation is, again, goes to the  
1441 wastebasket. As far as on paper, people think of them,  
1442 because their bank account was cleaned out, they couldn't pay  
1443 their mortgage, they lose their home, they can't run their  
1444 business, or what have you, because they no credit, they  
1445 can't get access to capital, et cetera. So let me tell you,  
1446 when you--when we allow you to do your job well, I think that  
1447 less and less of that does happen to our American public.

1448         So, with that, I only have time for perhaps one  
1449 question. I want to refer back to the--FTC recently released  
1450 a staff report on Internet of things. The Internet of things  
1451 refers to the ability of devices to connect to the Internet,  
1452 and send and receive data. As the report acknowledges, many  
1453 of these devices are vulnerable to being hacked. About 60  
1454 percent of web enabled devices have weak security, and that  
1455 is what has been reported.

1456         In September of 2013, the FTC took its first action  
1457 against an Internet of things company when it brought a

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1458 complaint against TRENDnet, a company that manufactures web-  
1459 enabled cameras, for misrepresenting the security of its  
1460 cameras. In that case, it was not personal information in  
1461 electronic form that was accessed, but rather live feeds from  
1462 the cameras, including the monitoring of babies.

1463         So, Ms. Rich, do you agree that reasonable security  
1464 measures include implementing procedures and practices that  
1465 limit the ability of hackers to remotely access control  
1466 Internet connected devices?

1467         Ms. {Rich.} Yes. You have touched on two things that  
1468 are very important to us about this bill. First, device  
1469 security. That is--it is because of our work on the Internet  
1470 of things that we realized that it is very important to  
1471 security devices so they can't--even regardless of the  
1472 personal information involved, they can't be taken over and  
1473 used in ways--for example, medical devices that--or  
1474 automobiles, which I discussed in my--at the beginning to  
1475 hurt consumers.

1476         And also, TRENDnet--our case against TRENDnet was an  
1477 example where it wasn't financial data that was exposed, it  
1478 was pictures of very private things happening in homes, and

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1479 that kind of sensitive information does need to be protected.

1480 Mr. {Cardenas.} Okay. Thank you. Ms. Rich, what type  
1481 of access control measures would limit the ability of hackers  
1482 to remotely accessing controlled devices, and how could  
1483 companies implement those measures to make consumers safer?

1484 Ms. {Rich.} We believe the legislation should actually  
1485 just include a reference to protecting device security in  
1486 order to make sure the--that is--that devices are protected  
1487 from that kind of interception.

1488 Mr. {Cardenas.} And also, generally, are the people who  
1489 have been attempting to hack, and it is my understanding that  
1490 it is in the millions and millions of attempts per year on  
1491 American companies, and on our government, et cetera, are  
1492 those hackers limited in their budgets? Do they seem to have  
1493 a limited budget per year, and they stop doing what they do,  
1494 and they wait until next year's budget?

1495 Ms. {Rich.} There are very sophisticated hackers out  
1496 there who are very motivated, and many of them aren't even in  
1497 this country. And many of them do these--they are so good at  
1498 what they do, they don't actually require a huge budget.

1499 Mr. {Cardenas.} Okay. I don't know if we could ever

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1500 even the playing field, but I would love to see that we  
1501 fortify you with the resources you need to protect us. Thank  
1502 you very much, Mr. Chairman.

1503 Ms. {Rich.} Can I just add something? I want to make  
1504 sure--I feel like I have been too modest in the way I  
1505 described our 55 cases, because those were completed cases  
1506 that ended in an order. And if we did include  
1507 investigations, and all of the--and closing letters, and all  
1508 of the activity we engage in that doesn't lead to a signed  
1509 order, there are hundreds of data security cases.

1510 Mr. {Burgess.} The Chair thanks the gentlelady for the  
1511 clarification. The Chair now recognizes Ms. Brooke from  
1512 Indiana. Five minutes for questions, please.

1513 Mrs. {Brooks.} And I want to thank all of the witnesses  
1514 for valuable time educating the public, educating all of us  
1515 on the proposed changes to further safeguard sensitive  
1516 consumer information by providing the timely to these  
1517 individuals. Also want to commend the Chairman on all the  
1518 work that has been done. As a new member to Energy and  
1519 Commerce, I know there has been a lot of work done over the  
1520 years, and, obviously, the growing nature of

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1521 cyberinfrastructure in all of our lives, it makes this so  
1522 very important.

1523 I have to tell you, we did--before the hearing today, in  
1524 2014 alone, the Indiana Attorney General's Office received  
1525 more than 370 data breach notifications, and more than 1,300  
1526 identity theft complaints in Indiana. Actually--that was,  
1527 actually, I thought, kind of low, considering many of us have  
1528 just received notification from our insurance company about  
1529 the breach in Indiana of potentially up to 80 million  
1530 customers.

1531 But I want to ask, from your perspective, Ms. Rich, at  
1532 the FTC, how does a national security standard in the draft  
1533 bill--wouldn't a national security standard help consumers,  
1534 in theory? And--because I am not hearing that you are  
1535 interested in a national security standard, but that, in  
1536 fact, we should continue to allow 47 to 50 different state  
1537 standards to be in place. Talk to me about a national  
1538 security standard, and what, you know, what your thoughts are  
1539 on that. Because I am not hearing that you are in favor of  
1540 that.

1541 Ms. {Rich.} We absolutely agree that a national



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1542 security standard would be helpful. It would make very clear  
1543 what the expectations are. It would fill the gaps, not--only  
1544 12 states have data security laws, even though 47 have data  
1545 breach laws, if I am up to speed on all the laws that have  
1546 passed. But we--

1547 Mrs. {Brooks.} Could you--

1548 Ms. {Rich.} We absolutely--

1549 Mrs. {Brooks.} --explain to us the distinction between  
1550 data security laws versus data breach laws?

1551 Ms. {Rich.} I just want to qualify what I was saying,  
1552 and then I definitely--

1553 Mrs. {Brooks.} Okay.

1554 Ms. {Rich.} --will. But we are concerned about a  
1555 national standard if it would water down protections that are  
1556 currently in place today, which is why we are suggesting some  
1557 modification to this discussion draft to strengthen it, so  
1558 that it wouldn't weaken the protections in place today.  
1559 Because if it preempts the state laws, and they--the main  
1560 thing there is health. To preempt state laws that provide  
1561 data security for health information, and that is already  
1562 provided now, then there won't--there would be fewer

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1563 protections for health information. So that is our concern.  
1564 But yes, in theory, we absolutely do support a national  
1565 standard.

1566 In terms of the difference between data security and  
1567 data breach, data security is protecting the data so there  
1568 isn't a breach. And, in fact, the FTC's focus has been  
1569 chiefly on that, not as much breach notification, in part,  
1570 because we don't have breach notification authority, except  
1571 in a narrow area. So data security is very, very important,  
1572 and that is why, right at the outset, I thanked the  
1573 Committee--the Subcommittee for including data security, and  
1574 not just data breach notification, which is, you know, after  
1575 the breach happens you tell consumers, but the horse is  
1576 already out of the barn.

1577 Mrs. {Brooks.} Can you explain--in your prepared  
1578 testimony you talked about it is critical that companies  
1579 implement reasonable security measures in order to prevent  
1580 data breaches. Can you elaborate? I was just Googling to  
1581 try to find out what, under FTC, reasonable security measures  
1582 mean. And I know that is a broad question, but yet--can you  
1583 please, you know, share with us what reasonable security

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1584 measures mean to the FTC? Because that is actually how you  
1585 determine which cases to take or not take. Is that not  
1586 really the crux of the issue?

1587 Ms. {Rich.} Yes. So we--in reasonableness, we are  
1588 referring to a bunch of factors which we have laid out again  
1589 and again. The sensitivity and volume of information  
1590 involved, you might want to have stronger security if you are  
1591 talking about, you know, Social Security Numbers, than simply  
1592 what, you know, size dress a person wears. The size and  
1593 complexity of the data operations, a small company won't need  
1594 to put as many protections in place if they have smaller data  
1595 operations. And the cost of available tools to secure data  
1596 and protect against known vulnerabilities. If there are not  
1597 available tools out there that a company can learn about and  
1598 use, it would not be--even if it could cause harm to  
1599 consumers, it would not be reasonable to expect them to have  
1600 known that.

1601 Now, those are factors to look at, but we also really  
1602 emphasize a process-based approach. Because if you undertake  
1603 a responsible process, you should be able to get to the  
1604 outcome of reasonable security. And also, process-based

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1605 approach is tech neutral, so put somebody in charge. I was  
1606 talking about this a bit earlier. Make somebody responsible.  
1607 Somebody should be lying awake at night, worrying about this.  
1608 You know, do a risk assessment. Put procedures in place to  
1609 address those risks, focusing on such areas as training.  
1610 Oversee your service provider. Periodically do evaluations  
1611 and updates of your program. If you do those procedural  
1612 things, and read all the information out there that provide  
1613 guidance on what is reasonable security, you should be able  
1614 to get to the reasonable security outcome.

1615       Mrs. {Brooks.} Thank you very much, and I look forward  
1616 to also learning, in the future, Mr. Chairman, how the FTC--  
1617 we are all focused on preventing the breach, enforcing if  
1618 there has not been adequate security. I would love to know  
1619 more about what we are doing to go after the hackers, and  
1620 whether we never hear that we ever catch the hackers. Thank  
1621 you, and I yield--

1622       Mr. {Burgess.} Chair thanks the gentlelady for that  
1623 observation. Chair recognizes the Ranking Member of the full  
1624 Committee, Mr. Pallone. Five minutes for questions, please.

1625       Mr. {Pallone.} Thank you, Mr. Chairman. I wanted to

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1626 ask Mr. Johnson these questions. I have a lot, so I am going  
1627 to try to go through it quickly, if you could answer quickly.  
1628 If this bill were to pass, Sections 201, 202, and 222 of the  
1629 Communications Act, and all associated regulations, which  
1630 include broad consumer privacy and data security protections,  
1631 would no longer be in effect with respect to security of data  
1632 in electronic form and breach notification.

1633 So, Mr. Johnson, can you walk us through some examples  
1634 of the types of consumer information that could have been  
1635 required to be protected by Internet service providers under  
1636 those sections? You know, first start, you know, could  
1637 Internet browsing history have been protected?

1638 Mr. {Johnson.} Well, I think the--that section, Section  
1639 222, has, for 18 years, been focused mostly on voice--on  
1640 telephone communications. As of last month the Commission's  
1641 reclassification of broadband Internet access service  
1642 expanded 222 to broadband providers, and there are presently  
1643 no specific rules in place that pertain to the broadband  
1644 service providers.

1645 But I think that underscores the value of having--of  
1646 public notice and comment rulemaking procedures to determine

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1647 what exactly--what precisely that requires in--

1648 Mr. {Pallone.} So would you say that Internet browsing  
1649 history could have been protected? Yes or no.

1650 Mr. {Johnson.} It could be, potentially.

1651 Mr. {Pallone.} All right. How about the unique  
1652 identifiers for wireless devices?

1653 Mr. {Johnson.} I think in--by unique identifiers, could  
1654 you tell me a little bit more?

1655 Mr. {Pallone.} Well, what about the--what about--I  
1656 mean, just tell me what you think would be protected, or  
1657 could be protected--

1658 Mr. {Johnson.} Well, what would--

1659 Mr. {Pallone.} --if it isn't at this point.

1660 Mr. {Johnson.} The bill does transfer some of the  
1661 protections for CPNI for call records data to the FTC, but  
1662 what it doesn't transfer is a number of other things that  
1663 pertain to the call service. And that is--this is just on  
1664 222. For instance, how many calls a person makes in a day,  
1665 what time they call, specific features of their call service,  
1666 call waiting, caller ID. And, importantly, things that are  
1667 not related to the telephone calls, but could be related to

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1668 the service that they have, their financial status, whether  
1669 they are low income. And that is just on 222. The bill also  
1670 would remove the existing--all of the existing protections  
1671 for cable and satellite and television viewing history, and  
1672 related information.

1673 Mr. {Pallone.} So let me just as a couple more. I know  
1674 there are only 2 minutes. If the bill were enacted, the FCC  
1675 would not be able to require Internet service providers to  
1676 protect sensitive customer information?

1677 Mr. {Johnson.} I think that is true. I think that is--

1678 Mr. {Pallone.} And the FCC would not be able to bring  
1679 enforcement actions against Internet service providers that  
1680 did not protect that information?

1681 Mr. {Johnson.} I think that is correct.

1682 Mr. {Pallone.} And as you read this bill--and this is  
1683 really the most important thing. As you read this bill, with  
1684 regard to Internet service providers, would there be any  
1685 protections for these types of customer info, beyond what is  
1686 listed as personal information, in the definition section?

1687 Mr. {Johnson.} That is--I think there would not be  
1688 beyond that definition, which is specific to financial harm

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1689 and fraud--

1690 Mr. {Pallone.} All right.

1691 Mr. {Johnson.} --and identity theft.

1692 Mr. {Pallone.} All right. Thanks so much.

1693 Mr. {Burgess.} Chair thanks the gentleman. Gentleman

1694 yields back his time. The Chair recognizes gentleman from

1695 Mississippi, Mr. Harper. Five minutes for questions, please.

1696 Mr. {Harper.} Thank you, Mr. Chairman, and thank you

1697 both for being here. Ms. Rich, I just have a question. The

1698 legislative draft calls for uniform data breach and

1699 information security requirements housed at the FTC,

1700 including leveling the playing field by bringing

1701 telecommunication, cable, and satellite providers under the

1702 FTC regime. In your opinion, is the FTC the appropriate

1703 agency to oversee data security for the Internet, how shall

1704 we say, ecosystem?

1705 Ms. {Rich.} We have been the lead agency on data

1706 security for now over 15 years, and we believe we should

1707 continue to provide that leadership, which is why we do want-

1708 -we appreciated nonprofits being in the bill, and we

1709 appreciated carriers in the bill. The bill even, though,



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1710 recognizes that others have a role to play. It allows the  
1711 states to enforce, even if--as it preempts, it allows the  
1712 states to enforce, and we would welcome that partnership with  
1713 the states.

1714 And as I mentioned before, we are--want to have common  
1715 carrier authority so we can protect consumers, but we would  
1716 be--we don't believe we should displace the FCC, or the  
1717 majority of the Commission don't believe we should displace  
1718 the FCC, so we would like to partner with them too in  
1719 protecting consumers in the carrier area.

1720 Mr. {Harper.} Thank you, Ms. Rich, and I yield back the  
1721 balance of my time.

1722 Mr. {Burgess.} Chair thanks the gentleman. Gentleman  
1723 yields back. The Chair recognizes the gentleman from North  
1724 Carolina, Mr. Butterfield. Five minutes for questions,  
1725 please.

1726 Mr. {Butterfield.} Thank you very much, Mr. Chairman.  
1727 Thank you for holding today's hearing. Thank you to the  
1728 witnesses for their testimony. This is absolutely an  
1729 important issue, Mr. Chairman, that many members of this  
1730 Subcommittee are familiar with. You know, we have worked

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1731 over the past few Congresses precisely on these concerns. As  
1732 members of the Subcommittee know, data breaches are occurring  
1733 in alarming numbers all across the country. Just in North  
1734 Carolina, our Attorney General estimates that about 6.2  
1735 million North Carolinians have been affected by data breaches  
1736 since 2005, that is over the last 10 years, so I am glad we  
1737 are addressing this issue today.

1738 Our good friend, and Chairman of the Subcommittee, Mr.  
1739 Rush, former Chairman of the Subcommittee Mr. Rush,  
1740 introduced a bipartisan bill entitled ``The Data  
1741 Accountability and Trust Act'', and during my time as Ranking  
1742 Member of this Subcommittee, I worked very closely with then  
1743 Chairwoman Bono, who I think I see here today, on the Secure  
1744 and Fortify Electronic Data Act. There is plenty of  
1745 precedent for finding bipartisan solutions on this subject.

1746 There are some issues with the discussion draft before  
1747 us today, and I encourage the majority to work with us so we  
1748 can finally produce meaningful legislation that will give  
1749 consumers the protections that they deserve, and businesses  
1750 they--that--and businesses. They certainly need to grow and  
1751 thrive.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1752           Let me just address one or two questions to the  
1753 witnesses. I may not take up the full 5 minutes, but I want  
1754 to discuss the APA rulemaking authority for just a moment.  
1755 One important thing about that authority is that it allows an  
1756 agency, such as yours, any agency with that authority, to  
1757 implement a law over time. It is particularly important for  
1758 laws concerning issues in which technical advances are  
1759 common, and fairly quick, to be flexible and agile. As  
1760 lawmakers, one thing we hate is having to revisit a law we  
1761 recently passed because it is already out of date.

1762           When Congress passed the Children's Online Privacy Law,  
1763 it allowed the FTC to amend the definition of personal  
1764 information through regular APA rulemaking procedures. Mr.  
1765 Johnson, can you explain how the FCC has been able to ensure  
1766 that Section 222 of the Act has stayed relevant at all times?  
1767 How has Section 222 been updated to deal with problems over  
1768 time, such as, most recently, when carriers were pre-  
1769 installing software onto devices that had security flaws?

1770           Mr. {Johnson.} Yes, sir, and I have already committed  
1771 to providing a detailed timeline of FCC's history with 222,  
1772 but I think that is a--your question is--gets right to the

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1773 heart of the value of having the flexibility and the agility  
1774 to adapt a statute to the changing technological landscape,  
1775 and also the changing public expectations and Congressional  
1776 expectations.

1777         So since the--since Section 222 was enacted in 1996,  
1778 entitled ``Privacy of Consumer Information'', there have been  
1779 a number of shifts. Obviously technologically, but also with  
1780 regard to Congressional expectation. The first was in 1999,  
1781 when, as part of the Wireless Communications Public Safety  
1782 Act, the Commission added location information into the  
1783 protected information under Section 222, and that is because  
1784 911 location accuracy is crucial.

1785         There was just a--tragically, a woman in Georgia who  
1786 made a 911 call on the border of a county line, and neither  
1787 of the two call centers knew where she was, and it cost her  
1788 her life, and this is something that we are trying to  
1789 improve. And now, under a new rule that was enacted--or was--  
1790 -the Commission voted on earlier this year, hopefully soon  
1791 the location accuracy will include being able to pinpoint a--  
1792 where a person is, which room in a multi-story building they  
1793 are in if they need help. But there are obviously incredibly

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1794 specific privacy concerns that come with that type of  
1795 location information.

1796 Mr. {Butterfield.} Absolutely.

1797 Mr. {Johnson.} So that is the type of thing that was  
1798 added in 1999, and it has been improved over time, and--  
1799 including the one that you mentioned, with regard to  
1800 information collected on mobile devices in 2013.

1801 Mr. {Johnson.} Right. All right. Let me go to Ms.  
1802 Rich. Ms. Rich, your testimony called for FTC to be granted  
1803 APA rulemaking authority to carry out the draft bill. Can  
1804 you give us an example, beyond COPA, where such limited  
1805 authority has allowed the FTC to deal with problems over  
1806 time? And, finally, are there any instances where not having  
1807 APA rulemaking authority inhibited the Commission's ability  
1808 to effectively deal with problems?

1809 Ms. {Rich.} The chief reason we want rulemaking  
1810 authority in this area is, as you note, to allow us to adapt  
1811 the consumer protections to make sure consumers are  
1812 effectively protected, even as technology changes. So the  
1813 Ranking Member mentioned geolocation as one type of  
1814 information that we wouldn't have thought to protect just--

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1815 not too many years ago, but another example is--we now know  
1816 that facial recognition--the information that is collected  
1817 through facial recognition is very sensitive, and we wouldn't  
1818 have thought of that. It was only recently that it was  
1819 recognized that Social Security Number alone could be used to  
1820 perpetrate identity theft, particularly in the case of  
1821 children, who don't have rich credit histories, and so it is  
1822 very easy to take the Social Security Number, and pass it off  
1823 as somebody else's.

1824         So those are some examples of information we wouldn't  
1825 have even known to protect a few years ago. And yes, we have  
1826 a number of instances where we have used our rulemaking to  
1827 not just adapt to change, but to respond when there were  
1828 needless burdens on businesses in a law. We did that in CAN-  
1829 SPAM. We used our rulemaking there. So there are a lot of  
1830 examples.

1831         Mr. {Butterfield.} Thank you very much, and thank you,  
1832 Mr. Chairman, for not calling time prematurely on the  
1833 witness. Thank you.

1834         Mr. {Burgess.} Chair thanks the gentleman. Chair  
1835 recognizes the gentleman from Oklahoma, Mr. Mullin. Five

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1836 minutes for questions, please.

1837 Mr. {Mullin.} Thank you, Mr. Chairman. Mr. Johnson, I  
1838 would like to spend most of my time, if not all my time,  
1839 visiting with you. Do you believe that a breach of  
1840 information involving a number of someone's calls could maybe  
1841 lead to theft or financial fraud? You mentioned about the  
1842 cell phones a while ago. Do you see this could maybe cause a  
1843 bigger problem down the road?

1844 Mr. {Johnson.} As--let me make sure I understand your  
1845 question. Could a breach of call data--

1846 Mr. {Mullin.} Of information. A breach of information  
1847 involving the number of someone's call. Could this lead to a  
1848 bigger problem?

1849 Mr. {Johnson.} I guess it--let me not engage in  
1850 hypotheticals, but I guess you could come up with some  
1851 scenarios in which the--a breach of non-financial telecom  
1852 information--

1853 Mr. {Mullin.} I mean, when you open that box, it leads  
1854 down a road that is unknown. Like you said, you are being  
1855 hypothetical on it.

1856 Mr. {Johnson.} Um-hum.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1857           Mr. {Mullin.} And I think there is a lot of work that  
1858 needs to be done. Now, obviously we want to protect the  
1859 consumer. It is tragic what you brought up a while ago. I  
1860 think most of us here read about that. We want to be able to  
1861 protect people. I mean, I live way out in the middle of  
1862 nowhere. My driveway is literally a mile long. The only way  
1863 I get cell phone coverage is--

1864           Mr. {Johnson.} Best way to--

1865           Mr. {Mullin.} --with the antenna that goes up my  
1866 chimney, and I would want someone to be able to respond.  
1867 There is no 911 address--

1868           Mr. {Johnson.} Right.

1869           Mr. {Mullin.} --where I live.

1870           Mr. {Johnson.} Right.

1871           Mr. {Mullin.} And I get that. But at the same time, I  
1872 don't want to open it up to exposing us to even a bigger  
1873 risk. All of us live in fear of fraud. The first time I had  
1874 experience with that, someone went to school on my Social  
1875 Security Number in California. At that time, I hadn't even  
1876 been to California, and I got a phone call wanting to know  
1877 what has happened. So it is something that we need to worry



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1878 about.

1879           Going on--you pointed out in your testimony, under the  
1880 proposed bill, the FCC could lose rulemaking authority over  
1881 data security. Has there been a--has the FCC effective--have  
1882 been effective in using the authority to protect consumers in  
1883 the 21st century?

1884           Mr. {Johnson.} I would say, sir, that this is a--this  
1885 will always be, as a cybersecurity--focus of my work is  
1886 cybersecurity, and has been for years, this will always be a  
1887 work in progress.

1888           Mr. {Mullin.} Right.

1889           Mr. {Johnson.} We are not going to solve this problem.  
1890 But I would say that I have--since I have been at the FCC, I  
1891 have been very impressed with the clarity of the expectations  
1892 that have developed, particularly on that--on Section 222 of--  
1893 -

1894           Mr. {Mullin.} Well, do you know how many regulatory  
1895 documents the FCC has published since '96?

1896           Mr. {Johnson.} I don't know. You mean new rules?

1897           Mr. {Mullin.} Yeah, new rules. Yeah.

1898           Mr. {Johnson.} We are committed to providing a full

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1899 list of not just rules, but activities.

1900 Mr. {Mullin.} Well, according to the Federal Registry,  
1901 the FCC has published nearly 14,000 rules since '96.

1902 Mr. {Johnson.} Pertaining to--

1903 Mr. {Mullin.} No.

1904 Mr. {Johnson.} Overall?

1905 Mr. {Mullin.} Overall. Do you know how many of those  
1906 pertain to our 21st century security issues that we are  
1907 having?

1908 Mr. {Johnson.} I would have a ballpark, but I--it  
1909 sounds like you--

1910 Mr. {Mullin.} Give me a ballpark.

1911 Mr. {Johnson.} --an answer.

1912 Mr. {Mullin.} I don't, because--seriously, we did a lot  
1913 of research trying to find it, and I really could not find  
1914 it. In fact, my follow-up was, could you provide the  
1915 information--

1916 Mr. {Johnson.} There have been a few rulemakings and  
1917 declaratory rulings on--specifically pertaining to 222, and  
1918 we will get you those exactly.

1919 Mr. {Mullin.} Are they being implemented right now?

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1920 Mr. {Johnson.} Yes, sir.

1921 Mr. {Mullin.} Do you know how long it is going to take?

1922 Mr. {Johnson.} Well, it is--I--it has been, and will

1923 always be, an ongoing process, but they are being

1924 implemented, and--

1925 Mr. {Mullin.} So it takes years to implement this?

1926 Mr. {Johnson.} Well, I don't know if I would--I think

1927 the premise of your question may be that it finishes at some

1928 point, and the--

1929 Mr. {Mullin.} Technology doesn't finish--

1930 Mr. {Johnson.} Right.

1931 Mr. {Mullin.} --and it seems like we are being very

1932 reactive, and we are not being proactive. We are responding

1933 to issues that happened years ago, and what we are trying to

1934 do is be in front of it.

1935 Mr. {Johnson.} I understand.

1936 Mr. {Mullin.} And if we continue to be reactive, how

1937 are we ever going to get ahead of the game?

1938 Mr. {Johnson.} Actually, I think you are absolutely

1939 right about the need to be proactive, and that is the value

1940 of having rulemaking authority.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1941           Mr. {Mullin.} And I agree with that, but the problem  
1942 that I have is, just recently, the FCC went all the way back  
1943 to 1930. So how is that being proactive? I mean, we are  
1944 wanting--you are wanting to keep the authority and have more  
1945 authority. We are wanting to move forward. We are wanting  
1946 to start being proactive, not reactive. You are making the  
1947 argument that you want to keep it, but the recent actions of  
1948 going all the way back to 1930 to a rule, how in the world,  
1949 with today's technology, is that being proactive?

1950           Mr. {Johnson.} You are referring to the open Internet--

1951           Mr. {Mullin.} Yes.

1952           Mr. {Johnson.} --order?

1953           Mr. {Mullin.} Of course I am.

1954           Mr. {Johnson.} I will stay disciplined and remain in my  
1955 lane on that. My focus is ensuring that the laws and  
1956 policies are in place to ensure that telephone calls go  
1957 through, that 911 calls have--

1958           Mr. {Mullin.} So let us finish on this, then. Do you  
1959 really believe the FCC can continue to be proactive, or do  
1960 you feel like you guys are being reactive?

1961           Mr. {Johnson.} I think, actually, it--we are not only

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1962 trying to be, but we are being proactive, and I can give you  
1963 two examples. One is--

1964 Mr. {Mullin.} No, it--my time is out, but I am just  
1965 going to tell you, from my opinion, it looks like we are  
1966 being extremely reactive. Mr. Chairman, thank you. Mr.  
1967 Johnson, thank you for your time. I yield back.

1968 Mr. {Burgess.} Chair thanks the gentleman. Gentleman  
1969 yields back. Chair recognizes the gentleman from Illinois.  
1970 Five minutes for questions, please, Mr. Kinzinger.

1971 Mr. {Kinzinger.} Well, thank you, Mr. Chairman, and  
1972 thank the witnesses for being here and spending a little time  
1973 with us today, and thank the Chairman for calling this  
1974 hearing. I probably won't take all 5 minutes. I basically  
1975 just have one question. I want to explore the issue of e-  
1976 mails, and in this draft bill, e-mail, data breach, et  
1977 cetera. I know in Florida there is a--their data breach and  
1978 security notification law actually requires--actually allows  
1979 for e-mail addresses, passwords, and--because in many cases  
1980 many people have the same e-mail and passwords into different  
1981 sites, as well as, you know, they use it for login into  
1982 something bigger.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

1983           Ms. Rich, in your testimony you note that within the  
1984 draft legislation the definition of personal information does  
1985 not protect some of the information which is currently  
1986 protected under state law, I would guess that would be part  
1987 of it with the e-mail. Could you please expand on which  
1988 elements that exist in the state law that would be most  
1989 important for us to consider within a Federal statute, and  
1990 would you include e-mail and passwords in that?

1991           Ms. {Rich.} I believe passwords are already in there in  
1992 various capacities, but yes, the most important elements we--  
1993 would be health, geolocation, and e-mail--and communications.  
1994 And as I--and device security. And as I mentioned earlier,  
1995 we believe--we have seen evidence that passport, driver's  
1996 license, and other government issued numbers could be used,  
1997 like Social Security Number, to perpetrate identity theft.  
1998 So that is my list.

1999           Mr. {Kinzinger.} Now--and let me ask--so let us talk a  
2000 little more about e-mail address and password. Could an e-  
2001 mail address and password combination, could that lead to  
2002 economic harm, and how could you see that happen? Is it more  
2003 than just somebody has access to your e-mail? Could that

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2004 lead to bigger economic harm if that is stolen?

2005 Ms. {Rich.} I can't spin out all the hypotheticals, but  
2006 e-mail address and password could get you into somebody's  
2007 account, allow you to read their e-mails, allow you to  
2008 communicate with perhaps accounts they have already set up  
2009 with some sort of automated, you know, I know when I interact  
2010 with accounts, I have often set it up, I know this is not a  
2011 great practice--security practice, so that I can pretty  
2012 quickly get on, it remembers me. So I think there are  
2013 probably a lot of scenarios we can spin out with e-mail and  
2014 password.

2015 Mr. {Kinzinger.} Okay. And do you have any ideas as  
2016 to, like, how do we reach that right balance of, you know,  
2017 finding out what can be breached, and there is a problem, and  
2018 also understand that we don't want to create legislation that  
2019 is entirely too burdensome to people?

2020 Ms. {Rich.} I think that the current draft already  
2021 covers a nice broad class of information, and we are very  
2022 complementary of the current draft. These were just a few  
2023 additional items that we believe could cause consumer harm if  
2024 they are intercepted by somebody else. And it is not an

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2025 endless list. These are a few things we believe should be  
2026 added.

2027 Mr. {Kinzinger.} Okay, great. And I will yield back a  
2028 minute and 40 seconds, Mr. Chairman.

2029 Mr. {Burgess.} Thank you. Chair thanks the gentleman,  
2030 gentleman yields back. Seeing there are no further members  
2031 wishing to ask questions, I do want to thank both of you for  
2032 your forbearance today. It has been very informative. Thank  
2033 you for participating in today's hearing. This will conclude  
2034 our first panel, and we will take a no more than 2 minute  
2035 recess to allow the staff to set up for the second panel.  
2036 Thank you, and this panel is dismissed.

2037 [Recess.]

2038 Mr. {Burgess.} Mr. Leibowitz, we will begin with you.  
2039 Five minutes for your opening statement, please.



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

2040 ^STATEMENTS OF JON LEIBOWITZ, PARTNER, DAVIS, POLK, AND  
2041 WARDWELL, LLP, CO-CHAIRMAN OF, AND ON BEHALF OF, THE 21ST  
2042 CENTURY PRIVACY COALITION; SARA CABLE, ASSISTANT ATTORNEY  
2043 GENERAL, OFFICE OF THE MASSACHUSETTS ATTORNEY GENERAL;  
2044 MALLORY DUNCAN, SENIOR VICE PRESIDENT AND GENERAL COUNSEL,  
2045 NATIONAL RETAIL FEDERATION; LAURA MOY, SENIOR POLICY COUNSEL,  
2046 OPEN TECHNOLOGY INSTITUTE, NEW AMERICA; AND YAEL WEINMAN,  
2047 VICE PRESIDENT, GLOBAL PRIVACY POLICY AND GENERAL COUNSEL,  
2048 INFORMATION TECHNOLOGY INDUSTRY COUNCIL

|

2049 ^STATEMENT OF JON LEIBOWITZ

2050 } Mr. {Leibowitz.} Thank you so much, Mr. Chairman.  
2051 Chairman Burgess, Ranking Member Schakowsky, members of the  
2052 panel, I want to thank you for inviting me to testify at this  
2053 important hearing. Chairman Burgess, you and I worked  
2054 together in the past on FTC related health care issues, and  
2055 you bring a wealth of experience to your new role. And  
2056 Ranking Member Schakowsky, you have been a leader on consumer  
2057 protection issues, going back to your work at Illinois Public

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2058 Action. Just as importantly, listening to this--to the panel  
2059 and the questions, I can just tell that both of you are  
2060 committed to finding practical solutions to real problems,  
2061 which is why you will certainly develop many bipartisan  
2062 initiatives going forward.

2063 Along with Mary Bono, your former Chairman, I serve as--  
2064 who is sitting over there, your former Chairman, I serve as  
2065 co-Chair of the 21st Century Privacy Coalition. Our group is  
2066 composed of the Nation's leading communications companies,  
2067 which have a strong interest in modernizing data security  
2068 laws to bolster consumers' trust in online services, and  
2069 confidence in the privacy and data security of personal  
2070 information. We are very supportive of the discussion draft  
2071 legislation and what it seeks to accomplish.

2072 Data security is an issue that I have cared deeply about  
2073 for many years, going back to my time as a commissioner on  
2074 the FTC. In fact, on behalf of the FTC, I testified before  
2075 this Subcommittee on this issue back in 2006. In testimony  
2076 then, and it was testimony for a unanimous Federal Trade  
2077 Commission, we urged Congress to enact strong data security  
2078 legislation that requires all businesses to safeguard

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2079 sensitive personal information, and gives notice to consumers  
2080 if there is a breach.'" And since then, as you know, the  
2081 need for legislation has only grown dramatically.

2082         You know all the statistics. Members have mentioned  
2083 them. In 2014 we saw a number of data breaches. Just this  
2084 morning in the Washington Post I read about a hack that may  
2085 have exposed 11 million people, Primera customers, and their  
2086 sensitive personal information. And when these breaches  
2087 happen, they typically expose sensitive information. That is  
2088 what all of the members had said in the first panel, how  
2089 important that information is to consumers.

2090         Data breaches resulting in the exposure of personal  
2091 information can result in substantial harm to consumers.  
2092 Companies that fail to take responsible measures to protect  
2093 this information need to be held accountable. And that is  
2094 why our coalition commends Representatives Blackburn and  
2095 Welch, for releasing the Data Security and Breach  
2096 Notification Act draft. The discussion draft contains  
2097 elements we believe are essential for effective data breach  
2098 and data security legislation. Let me highlight just a few  
2099 of them now.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2100           First, the draft includes both breach notification  
2101 standards and substantive data security requirements. While  
2102 notifying consumers that a breach has occurred is important,  
2103 it is ultimately of little value if companies are not  
2104 required to put into place reasonable data security systems  
2105 to protect consumers' sensitive information. In the first  
2106 instance, these security requirements have to be strong, they  
2107 should be clear, and they should be flexible to give  
2108 consumers confidence, while giving companies a fair  
2109 opportunity to comply with the law.

2110           And some of this--I was listening to the back and forth  
2111 with Mr. Pallone and the two witnesses earlier. It seems to  
2112 me that some of the information they were talking about that  
2113 might not be covered by the FCC could be covered, and would  
2114 be covered--currently would be covered by the FTC in its UDAP  
2115 statute, its Unfair and Deceptive Act or Practice statutes.  
2116 We can talk about that more in the Q and A.

2117           Second, the bill would replace the ever-changing  
2118 patchwork of 47 different breach laws with a single Federal  
2119 standard. A single Federal law reflects the reality that  
2120 data is in cabin within individual states, but inherently

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2121 moves in interstate commerce. Consumers in every part of the  
2122 country are entitled to the same robust protections, and  
2123 companies are entitled to a logical and coherent compliance  
2124 regime, and only a bill with state law preemption can  
2125 accomplish that.

2126         Third, the draft smartly puts enforcement authority in  
2127 the hands of America's top privacy cop, the Federal Trade  
2128 Commission, while also empowering each state's Attorney  
2129 General to enforce the Federal standard. The Federal Trade  
2130 Commission, under both Democratic and Republican leadership,  
2131 has, for many years, been our country's foremost protector of  
2132 data security. The FTC has brought, and you heard this  
2133 before from Jessica Rich, brought more than 50 data security  
2134 enforcement actions in the last 10 years. And the draft  
2135 would give the FTC more powerful tools, including fining  
2136 authority, which it doesn't have now, to protect consumers  
2137 and punish companies for inadequate protections. And  
2138 moreover, by empowering state AGs to enforce the new Federal  
2139 standard, the bill will ensure there are no gaps in  
2140 enforcement. I think this bill is better for consumers than  
2141 current law.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2142           Mr. Chairman, given the President's strong endorsement  
2143 for data breach legislation, as well as the growing support  
2144 of the FTC, we believe you are poised to enact a law that  
2145 provides strong protections for consumers, and holds  
2146 companies to a single robust standard. In short, this  
2147 measure would provide a practical solution to a real problem  
2148 facing all Americans, and I commend members of this  
2149 subcommittee for working on a bipartisan legislation.

2150           With your permission, I ask that my full statement be  
2151 put into the record. Thank you.

2152           [The prepared statement of Mr. Leibowitz follows:]

2153 \*\*\*\*\* INSERT C \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

2154 Mr. {Burgess.} Without objection, so ordered.

2155 Ms. Cable, welcome to the subcommittee. You are

2156 recognized. 5 minutes for your opening statement, please.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

2157 ^STATEMENT OF SARA CABLE

2158 } Ms. {Cable.} Thank you. Good morning, Chairman  
2159 Burgess, Ranking Member Schakowsky, distinguished members of  
2160 the subcommittee. Thank you for inviting me here today to  
2161 testify. My name is Sara Cable, and I am an Assistant  
2162 Attorney General with the Office of the Massachusetts  
2163 Attorney General, Maura Healey, and I am here today on behalf  
2164 of my office to present some of our concerns with the bill.

2165 My comments today are informed by my office's experience  
2166 enforcing Massachusetts data security and breach laws, which  
2167 are regarded as among the strongest in the country. My  
2168 office works hard to use those laws to protect our residents,  
2169 and we believe that our consumers are better protected as a  
2170 result. We are encouraged that the Subcommittee recognizes a  
2171 critical necessity of data security and breach protections.  
2172 We share this goal. This is our most sensitive information.  
2173 Yours, mine, our children, our parents, our co-workers, our  
2174 friends. We are all impacted, and we all deserve robust  
2175 protections.



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2176           We understand Federal standardization is the thrust of  
2177 this bill. We do, however, have serious concerns that the  
2178 standards set by this bill are too low, preempt too much, and  
2179 hamstring the ability of my office, and that of the other  
2180 Attorney General offices across the country, to continue our  
2181 important work of protecting our consumers. It is our  
2182 concern that this bill would--as drafted would set aside the  
2183 robust consumer protections that already exist in  
2184 Massachusetts and many other states, and replace them with  
2185 weaker protections at a time when strong protections are  
2186 imperative.

2187           My first point focuses on the bill's proposed data  
2188 security standard. We agree strong data security standards  
2189 are essential. This is how breaches are prevented. This is  
2190 how the whole business of providing notice of breaches can be  
2191 prevented. The bill would require ``reasonable security  
2192 measures and practices.'' Our concern, however, is that it  
2193 does not specify or delineate precisely what practices or  
2194 measures are required. It may be true reasonableness is a  
2195 useful standard in general, but it--standing alone, it is not  
2196 particularly useful when trying to understand what actual

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2197 practices and measures are required.

2198           We think that the only way reasonable can be determined  
2199 under the bill as drafted will be through piecemeal  
2200 protracted litigation, and the standard will differ from case  
2201 to case and company to company. It will cause needless  
2202 confusion, expense, and risk for companies, who are forced to  
2203 guess what measures and practices will ultimately be  
2204 considered by--considered reasonable.

2205           We think Massachusetts has the better approach. It has  
2206 in place data security regulations that are tech neutral,  
2207 process-oriented, and, importantly, describe the basic  
2208 minimum components of a reasonable data security program.  
2209 Some of those components are--you have heard them from the  
2210 FTC earlier today, conducting a risk assessment, developing,  
2211 implementing, and maintaining a written information security  
2212 program, establishing computer security controls, and many  
2213 others. The Massachusetts regulations are consistent with  
2214 those currently in place under Gramm-Leach-Bliley and HIPAA.  
2215 We believe that they provide stronger protections to our  
2216 consumers. Our view is that the bill as drafted would erase  
2217 these strong protections, and, we believe, would ultimately

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2218 be harmful to consumers.

2219           My second point concerns the scope of the bill's  
2220 preemption. Put simply, we think it is too broad. It would  
2221 restrict my office's ability to enforce our own consumer  
2222 protection laws. It would prevent innovative states from  
2223 legislating in this field in response to purely local  
2224 concerns, for example, a breach involving a Massachusetts  
2225 company and Massachusetts residents only. Under my  
2226 interpretation, I think the bill might even go further, and  
2227 it might possibly restrict states from enforcing, for  
2228 example, criminal laws relating to the unauthorized access of  
2229 electronic communications. It might possibly also preempt a  
2230 state's ability to enforce the security obligations under  
2231 HIPAA, an enforcement power given to the states under the  
2232 High Tech Act. These laws, and others, relate to the issue  
2233 of unauthorized access to data in electronic form, and under  
2234 the current language of the bill, we believe the--our state's  
2235 ability to enforce those laws would be preempted.

2236           Finally, the bill hamstringing my office's ability to  
2237 protect Massachusetts consumers. Currently, under Mass law,  
2238 we get notice of any breach involving one or more

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2239 Massachusetts residents. From January 2008 through July 31,  
2240 2014 Massachusetts has received notice of over 8,600  
2241 breaches, impacting over five million Massachusetts  
2242 consumers. That is in Massachusetts alone. Under this bill,  
2243 we would receive none of those notices. We believe this is a  
2244 critical omission in the bill. It restricts our ability to  
2245 enforce the requirements of the bill, and we believe  
2246 ultimately it will make our job of protecting our consumers a  
2247 lot more difficult.

2248           And with that, I thank the Committee for their--  
2249 Subcommittee for their efforts, and for inviting me today.  
2250 Thank you very much.

2251           [The prepared statement of Ms. Cable follows:]

2252 \*\*\*\*\* INSERT D \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

2253 Mr. {Burgess.} The Chair thanks the gentlelady.

2254 Mr. Duncan, welcome to the Subcommittee. You are

2255 recognized 5 minutes for the purpose of an opening statement.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

2256 ^STATEMENT OF MALLORY DUNCAN

2257 } Mr. {Duncan.} Thank you, Dr. Burgess, Ranking Member  
2258 Schakowsky, members of the Committee for inviting us here  
2259 today, and particularly Congressmen Blackburn and Welch for  
2260 their efforts to produce this draft legislation. Thank you  
2261 too for the courtesy and consideration you and your staffs  
2262 have shown to us and our members over the past many months.  
2263 The result of those discussions, and undoubtedly many more,  
2264 is a working draft that is significantly better than  
2265 introducing--legislation introduced in prior Congresses. We  
2266 look forward to continue working with you to help turn the  
2267 draft into a legislative product that will provide increased  
2268 security and protection for consumers, ameliorate burdens on  
2269 business, and establish meaningful and reasonable standards  
2270 for all.

2271 I would like to set out three or four principles that  
2272 have guided our work. Number one, breaches affect everyone.  
2273 Every entity that has a significant breach of sensitive data  
2274 should have an obligation to make that fact publicly known.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2275 Public notice serves two goals. First, it provides consumers  
2276 with information they might be able to use to better protect  
2277 themselves from identity theft. Second, the fear of public  
2278 notice strongly incentivizes companies to improve their  
2279 security. Both goals are important. Enacting legislation  
2280 that exempts some entities from public notice, or that  
2281 perpetuates notice holes that would allow companies to hide  
2282 breaches undermines both.

2283 Two, if one is a mid-sized regional company, or an e-  
2284 commerce startup struggling with the consequences of a  
2285 breach, the existing morass of inconsistent laws are little  
2286 more than traps for the unwary. We need Federal preemption  
2287 that works.

2288 Three, if we are going to preempt the state laws, we owe  
2289 it to the states, and to their citizens, not to adopt a weak  
2290 law. We should seek legislation that reflects a strong  
2291 consensus of the state laws and carefully strengthen them  
2292 where doing so supports the other two principles.

2293 And four, if we are to specifically adopt data security  
2294 standards, they should not be defined technical standards,  
2295 and they must be comprehensible and actionable from the

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2296 perspective of the companies against whom they will apply.

2297         With those principles in mind, I would like to address a  
2298 few areas of the draft. One, there is not good reason why a  
2299 breach law should apply a high standard for reporting against  
2300 some companies, such as retailers, restaurants, dry cleaners,  
2301 and other small businesses, while requiring little or no  
2302 notice from some of the biggest firms in America holding the  
2303 same sensitive data, be they cloud services like Apple, or  
2304 payment processors like Hartline when they suffer a breach.  
2305 Not only does the draft excuse them from general public  
2306 notice, undermining security incentives, the draft allows big  
2307 businesses to shift liability for their breaches onto smaller  
2308 business. This is worse than what exists under the state  
2309 laws. It must be fixed.

2310         Two, preemption. In general, the preemption language in  
2311 the draft is much better than in previous Congress's bills.  
2312 If the notice holes are filled, it could replace the  
2313 conflicting welter of state requirements with a single strong  
2314 law. The one area for concern is the clause that  
2315 specifically excludes some laws from preemption. Federal  
2316 jurisprudence suggests that when that is done, the entire



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2317 preemption clause could be placed in jeopardy.

2318           Three, there are portions of the draft that are  
2319 inconsistent with the considered strong consensus of state  
2320 laws. For example, we know of no state law that expressly  
2321 exempts communication service providers, and that would allow  
2322 them, even when they know they have a serious breach, to get  
2323 away with providing no notice to anyone at all. That is a  
2324 notice hold you could drive a truck through.

2325           Finally, as to data security, when the FTC applies  
2326 generalized standards to businesses, such as unfairness or  
2327 deception, as--or, as should be proposed here, reasonable  
2328 security standards, they are enforced under Section 5 of the  
2329 FTC Act, which calls for a cease and desist order before  
2330 penalties can be imposed. The law allows businesses to  
2331 understand what is intended by the vague standards before  
2332 they are made subject to massive penalties.

2333           While going directly to damages might be appropriate for  
2334 an objective on/off requirement, like giving notice within 30  
2335 days, it does not make sense when the legal requirement is  
2336 simply to do something reasonable, or not to be unfair. That  
2337 is the way the Commission has worked very effectively for

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2338 over 100 years. Congress should not leave companies subject  
2339 to fines for practices they could not know in advance, or  
2340 unreasonable in the eyes of the FTC. That must be remedied.

2341 Thank you for the opportunity to speak today. We look  
2342 forward to working with you to craft a strong, effective, and  
2343 fair law.

2344 [The prepared statement of Mr. Duncan follows:]

2345 \*\*\*\*\* INSERT E \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

2346 Mr. {Burgess.} The Chair thanks the gentleman.

2347 The Chair now recognizes Ms. Moy. Five minutes for your

2348 opening statement, please.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

2349 ^STATEMENT OF LAURA MOY

2350 } Ms. {Moy.} Thank you. Good morning, Dr. Burgess,  
2351 Ranking Member Schakowsky, distinguished members of the  
2352 Subcommittee. Thank you for your shared commitment to  
2353 addressing data security and data breaches, and for the  
2354 opportunity to testify on this important issue.

2355 Consumers today share tremendous amounts of information  
2356 about themselves. Consumers benefit from sharing  
2357 information, but they can also be harmed if that information  
2358 is compromised. For that reason, 47 states, and the District  
2359 of Columbia, all currently have data breach laws on the  
2360 books, and several states have specific data security laws.  
2361 Many states also use general consumer protection provisions  
2362 to enforce privacy and security.

2363 To preserve strong state standards, and the ability to  
2364 protect protections to the needs of their own residents, a  
2365 Federal law should set a floor for disparate state laws, and  
2366 not a ceiling. But, in the even that Congress seriously  
2367 considers broad preemption, the new Federal standard should

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2368 strengthen, or at least preserve, import protections that  
2369 consumers currently enjoy. This bill, however, would weaken  
2370 consumer protections in a number of key ways. These concerns  
2371 must be addressed, and if they are not addressed, it would be  
2372 better for privacy to pass no bill than to pass this bill as  
2373 currently drafted. I will highlight five particular  
2374 concerns.

2375         First, the bill's definition of personal information is  
2376 too narrow. The bill threatens to weaken existing  
2377 protections by eliminating state laws covering information  
2378 that falls outside of its narrow terms. For example, health  
2379 information, as others have mentioned, falls outside this  
2380 bill's definition of personal information. As a result,  
2381 passing this bill would mean eliminating breach notification  
2382 coverage of that information in Florida, Texas, and seven  
2383 other states.

2384         Second, this bill would condition breach notification on  
2385 a narrow financial harm trigger. Data breaches may lead to a  
2386 number of serious harms beyond merely those that are  
2387 financial in nature, one reason why seven states in the  
2388 District of Columbia have no harm trigger at all, and why

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2389 triggers in another 26 states are not specifically financial  
2390 in nature.

2391 Third, the bill's general reasonableness security  
2392 standard would replace the more specific security standard  
2393 set forth in many state laws, and the FCC's rules  
2394 implementing the Communications Act. Some states have  
2395 specific data security standards in place, and the FCC's CPNI  
2396 rules require carriers to train personnel on CPNI, have an  
2397 express disciplinary process in place for abuses, and certify  
2398 on an annual basis that they are in compliance with the  
2399 rules. This bill threatens to eliminate these carefully  
2400 designed security requirements, replacing them with a general  
2401 reasonableness standard.

2402 Fourth, this bill would supersede important provisions  
2403 of the Communications Act that protect telecommunications,  
2404 cable, and satellite customers. Consumers rely on the  
2405 Communications Act, and the FCC's implementation of it, to  
2406 protect the very sensitive information that they cannot avoid  
2407 sharing with the gatekeepers of communications networks. But  
2408 this bill threatens to replace those protections with weaker  
2409 standards. In addition, this bill would eliminate

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2410 protections for the viewing histories of cable and satellite  
2411 subscribers that fall outside the bill's definition of  
2412 personal information. The proposed reduction of FCC  
2413 authority could not come at a worse time for consumers, right  
2414 as the FCC is poised to apply its Title 2 authority over data  
2415 security and breach notification to broadband.

2416         The bill strives to eliminate FCC authority only insofar  
2417 as it relates to information security or breach notification,  
2418 while preserving the FCC's authority to set privacy controls.  
2419 But privacy rules that give consumers the right to control  
2420 their information are of greatly diminished value when there  
2421 are no security standards to protect against unauthorized  
2422 access.

2423         Fifth, the bill could eliminate a wide range of existing  
2424 consumer protections that may be used to enforce both privacy  
2425 and data security. The bill is designed to preempt state law  
2426 and supersede the Communications Act only with respect to  
2427 information security and breach notification, but in practice  
2428 it would be exceedingly difficult to draw the line between  
2429 information security and breach notification on the one hand,  
2430 and privacy and general consumer protection on the other.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2431           We are not unequivocally opposed to the idea of Federal  
2432 data security and breach notification legislation, but any  
2433 such legislation must strike a careful balance between  
2434 preempting existing laws and providing consumers with new  
2435 protections. The draft Data Security and Breach Notification  
2436 Act of 2015 falls short of that balance, but we at the Open  
2437 Technology Institute do appreciate your commitment to  
2438 addressing these issues, and we hope to work with you to  
2439 strengthen the bill and strike a better balance as it moves  
2440 forward.

2441           Thank you, and I look forward to your questions.

2442           [The prepared statement of Ms. Moy follows:]

2443 \*\*\*\*\* INSERT F \*\*\*\*\*



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

2444 Mr. {Burgess.} Thank you for your testimony.

2445 Ms. Weinman, thank you for--welcome to the Subcommittee.

2446 You are now recognized for 5 minutes for the purpose of an

2447 opening statement.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

2448 ^STATEMENT OF YAEL WEINMAN

2449 } Ms. {Weinman.} Thank you. Chairman Burgess, Ranking  
2450 Member Schakowsky, and members of the Subcommittee, thank you  
2451 for the opportunity to testify today. My name is Yael  
2452 Weinman, and I am the Vice President for Global Privacy  
2453 Policy and the General Counsel at the Information Technology  
2454 Industry Council, known as ITI. Prior to joining ITI in  
2455 2013, I spent more than 10 years as an attorney at the  
2456 Federal Trade Commission, most recently as an attorney  
2457 advisor to Commissioner Julie Brill.

2458 The 60 technology companies that ITI represents are  
2459 leaders and innovators in the information and communications  
2460 technology sector. These are companies that are committed to  
2461 the security of their customers' information. The reality  
2462 remains, however, that while organizations race to keep up  
2463 with hackers, these criminals attempt to stay one step ahead.  
2464 And when a network is compromised, and personal information  
2465 has been breached, individuals may be at risk of identity  
2466 theft or financial fraud.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2467 Consumers can take steps to protect themselves from  
2468 identity theft or other financial fraud following a data  
2469 breach. Federal breach notification legislation would put  
2470 consumers in the best possible position to do so. In the  
2471 written testimony I provided to you in advance of this  
2472 hearing, I included the set of nine principles that ITI  
2473 recommends be included in Federal breach notification  
2474 legislation. The draft legislation that is the subject of  
2475 this hearing reflects a number of these important principles.  
2476 I highlight three.

2477 First, the legislation preempts the existing patchwork  
2478 in the United States of 51 different regimes. That is 47  
2479 states and four territories. Such preemption is critical in  
2480 order to streamline notices and avoid consumer confusion.  
2481 Second, the legislation's timeline for notification  
2482 recognizes that notification can only take place once an  
2483 organization determines the scope of the data breach, and has  
2484 remedied vulnerabilities. The timeline included in the draft  
2485 legislation also permits the necessary flexibility to enable  
2486 companies to delay notification at the request of law  
2487 enforcement. Third, the legislation does not require

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2488 notification if data is unusable, recognizing that power  
2489 security tools have been developed that avoid risks if data  
2490 has been compromised.

2491 ITI appreciates how these three important elements are  
2492 incorporated into the draft legislation. Greater clarity and  
2493 discussion is needed, however, in a number of areas, and I  
2494 highlight three today.

2495 First, the description of the level of risk, and the  
2496 potential ensuing harm that would trigger the notification,  
2497 appears to be broad. The threshold of reasonable risk,  
2498 combined with the phrase economic loss or economic harm could  
2499 lead to over-notification. It is unclear how economic loss  
2500 or economic harm is being distinguished from the phrase  
2501 financial fraud that also appears in the text. Year after  
2502 year identity theft tops of the list of consumer complaints  
2503 reported to the FTC, and identity theft or financial fraud  
2504 are the appropriate triggers for providing consumer notice.  
2505 And, upon notification, consumers can then take the necessary  
2506 steps to protect themselves.

2507 Second, with regard to the timing of notification, as  
2508 currently written, the timeline for a covered entity to

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2509 notify consumers if a third party suffered a data breach is  
2510 unclear. The third party needs to remedy vulnerabilities and  
2511 restore its systems before the covered entity provides  
2512 notice. The draft should be clarified that the third party  
2513 will be given the opportunity to restore its system prior to  
2514 the point in time that the covered entity is required to  
2515 provide notice to consumers.

2516 Third, the maximum penalty amounts set in the draft  
2517 legislation are high, \$2.5 million maximum for each violation  
2518 of the data security section, and a \$2.5 million maximum for  
2519 notice related violations arising from a single incident.  
2520 These amounts appear punitive, and do not seem to reflect  
2521 that an organization that suffered a data breach, in most  
2522 cases, is the victim itself of criminal hackers.

2523 As ITI and its member companies continue to study the  
2524 draft, and as we gather feedback, we look forward to sharing  
2525 that with members of the Committee. Thank you, and I am  
2526 happy to answer any questions.

2527 [The prepared statement of Ms. Weinman follows:]

2528 \*\*\*\*\* INSERT G \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

2529 Mr. {Burgess.} The Chair thanks the gentlelady, thanks  
2530 all the witnesses for your forthright testimony today. We  
2531 will move into the question and answer portion of this panel.  
2532 Recognize myself for 5 minutes for questions.

2533 And, Mr. Leibowitz, if I could, let me start with you.  
2534 You are familiar with the draft legislation before us. Do  
2535 you think consumers would be more or less protected with  
2536 respect to information held by telecom providers under this  
2537 draft?

2538 Mr. {Leibowitz.} I think--look, my view is that  
2539 consumers--if this bill were to pass tomorrow, be signed into  
2540 law, consumers would be in a better position, and let me just  
2541 tell you why I think that.

2542 First of all, the, you know, the FTC, as the witnesses--  
2543 both witnesses acknowledged in the previous panel, has been a  
2544 leader, America's top consumer protection cop, including in  
2545 the data security area, with more than 50 cases, and hundreds  
2546 of investigations. There is an emerging consensus, and I  
2547 think this is critically important, that the most appropriate  
2548 way to protect personal information, and this is at the core

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2549 of your bill, is with strong, but flexible, data security  
2550 standards. It is not with prescriptive rules.

2551 And there is also an ever-changing patchwork of state  
2552 legislation. Now, I have seen legislation, when I was at the  
2553 FTC, that sometimes took state AGs entirely out of the  
2554 business of enforcing the law. You do not do that, and I  
2555 think that is critically important, because you want state  
2556 AGs to be a top cop here. And nobody wants to see any gaps  
2557 in the legislation. I do not read this legislation as having  
2558 any gaps, but we certainly want to work with you, if that  
2559 seems to be the--if--to tweak--to do some tweaking, if that  
2560 is necessary.

2561 Mr. {Burgess.} Well--and I thank you for that response.  
2562 So just in general, you--with your experience as Chairman of  
2563 the Federal Trade Commission, you would interpret this draft  
2564 legislation as strengthening consumer protections across the  
2565 board?

2566 Mr. {Leibowitz.} I do. And let me just come back to  
2567 one question, because it came back in the--came up in the  
2568 first panel, about the issue dual jurisdiction. And I  
2569 understand that sometimes the FTC and the FCC work together,

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2570 and sometimes they can work together as a--very  
2571 collaboratively.

2572 But just as I believe that the FTC should be the sole  
2573 Federal enforcer of data security, because I think it does a  
2574 really good job, and it has expertise, and it is concentrated  
2575 on that for decades, really going back to the Fair Credit  
2576 Reporting Act passed in the 1970s, you know, I also wouldn't  
2577 want to see, for example, the FCC go into the business of  
2578 spectrum auctions, right? That is something that the FCC  
2579 does really well. It is a terrific agency at that, and, you  
2580 know, I think you should just let each agency play to its  
2581 strengths and to its expertise. Shouldn't be any gaps in the  
2582 legislation, I don't believe there are, but that is the way,  
2583 I think, to sort of improve the protections that companies  
2584 have to have, and ultimately improve the lives of consumers.

2585 Mr. {Burgess.} Thank you, sir. Ms. Weinman, let me  
2586 just ask you, you are a former FTC attorney advisor. Tell me  
2587 what you see is the difference between privacy and security.

2588 Ms. {Weinman.} Thank you for the question. Privacy  
2589 relates to how an organization uses data, with whom it  
2590 chooses to disclose that data. Security relates to the



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2591 underlying security of that information, and the access to  
2592 which would be unauthorized. That, to me, is the key word in  
2593 distinguishing between privacy and data security.

2594 Mr. {Burgess.} And is that difference important for the  
2595 Subcommittee to consider in its drafting of the bill?

2596 Ms. {Weinman.} Absolutely. I think that, in some ways,  
2597 privacy and data security are often conflated. But I think,  
2598 with respect to this bill, you do a good job of separating  
2599 out the two, and focusing on data security. So I think it is  
2600 something to keep in mind, because there is often conflation,  
2601 but I think it is important to keep those two concepts  
2602 distinguished, and I think this bill does a good job of that.

2603 Mr. {Burgess.} Mr. Leibowitz, let me come back to you  
2604 just on that issue of privacy and security--data security  
2605 requirements. Do you feel the bill is doing an adequate job  
2606 in that regard?

2607 Mr. {Leibowitz.} I do, Mr. Chairman, and, you know, you  
2608 can look at them as sort of Venn diagrams with a slight  
2609 overlap. You can look at them as--along the lines of a  
2610 continuum. But I think you can separate them. I think you  
2611 do a very good cut in your discussion draft. And you

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2612 concentrate on what Mr. Welch said, and Mr. Cardenas, and  
2613 others had said, is the most--and Ms. Brooks said is the most  
2614 important information here is the personally identifiable  
2615 information. It is what the hackers really care about,  
2616 right? And that is what you need to have the highest level  
2617 of protection for, data security, and you need to give  
2618 notification to consumers.

2619 Mr. {Burgess.} Very good. My time has expired. I will  
2620 yield back. I just want to--time for questions is limited,  
2621 and I do have some questions that I am going to submit, and  
2622 ask for a written response, Ms. Cable, in particular for you,  
2623 and some of the issues that happened around the High Tech Act  
2624 of Massachusetts, but I will do that in writing.

2625 And I will recognize Ms. Schakowsky. Five minutes for  
2626 questions, please.

2627 Ms. {Schakowsky.} Before--because he has a bill on the  
2628 floor, I am going to yield right now out of order, Mr.  
2629 Kennedy, for questions.

2630 Mr. {Kennedy.} I want to thank the Ranking Member for  
2631 the generosity, and, Mr. Chairman, thank you for calling the  
2632 hearing. To all of our witnesses today, thank you for

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2633 spending the time, thank you for your testimony. I had the  
2634 pleasure of introducing Ms. Cable this morning from  
2635 Massachusetts, so thank for being here, ma'am. And I wanted  
2636 to get your thoughts, as an enforcement lawyer from  
2637 Massachusetts--we have heard a number of criticisms of the  
2638 draft bill today, but I would much rather focus on how we can  
2639 make this bill stronger, or the data security and breach  
2640 notification aspects a bit better.

2641         So, in your opinion, ma'am, what are some of the most  
2642 critical data security standards in Massachusetts law that  
2643 you believe are not represented within the framework of the  
2644 proposed bill?

2645         Ms. {Cable.} Sure, of course, and I will echo what was  
2646 previously said by the FTC, and I alluded to in my testimony.  
2647 You know, this is a framework that includes, at the first  
2648 step, an evaluation and assessment. What personal  
2649 information does the company have, where is it, how do they  
2650 use it? What are the reasonably foreseeable risks to that  
2651 information, both internal and external? It is the process  
2652 of taking stick and evaluating what the risks are that is not  
2653 reflected in this current draft of the bill that I believe is

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2654 critically necessary. And you can see that reflected in  
2655 Gramm-Leach-Bliley standards, and I believe the HIPAA  
2656 security rule as well.

2657         Stemming from that process are, then, the safeguards  
2658 that need to be put in place. Again, Massachusetts law  
2659 leaves open, and gives companies some flexibility, what are  
2660 the specific safeguards. They include things like  
2661 restricting employee access to information on an--on a  
2662 business need basis only. It includes simple things you  
2663 might not even think about, changing passwords when someone  
2664 leaves the company, for example.

2665         There is--computer security systems need to be paid  
2666 careful attention to because of the volume of data they can  
2667 store, and the many points of access to that data. So  
2668 perimeter security, such as firewalls, anti-virus protection,  
2669 software patches. The Massachusetts data security  
2670 regulations are technology neutral. They leave open, and  
2671 they contemplate changes in technology and improvement in  
2672 procedures, but they establish a minimum concept of  
2673 protecting your computer's security network. There are many  
2674 more, but, you know, I think it is a process oriented--it

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2675 requires a company to take an introspective look at itself  
2676 and its information, and it is an iterative, evolving  
2677 process, and I think that is what is important about it.

2678 Mr. {Kennedy.} So, given that, Ms. Cable, do you think  
2679 that should be--or that framework should be a national  
2680 benchmark, or what additional requirements do you think you  
2681 could suggest to further enhance the protection of consumers'  
2682 data?

2683 Ms. {Cable.} Well, I think it has been--it was  
2684 suggested in first panel, and it is the concept of FTC  
2685 rulemaking authority. And I think that is something that--

2686 Mr. {Kennedy.} Um-hum.

2687 Ms. {Cable.} --that our office would support a closer  
2688 look at.

2689 Mr. {Kennedy.} And maybe that is the answer to this  
2690 next question, but how can we ensure that the data security  
2691 standard is responsive to rapidly evolving technologies and  
2692 increasingly sophisticated cyber attacks?

2693 Ms. {Cable.} I think, you know, giving the FTC the  
2694 authority and flexibility to, you know, enact regulations  
2695 that are sufficiently flexible and responsive is one way to

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2696 do it. And, you know, I think we--I haven't heard anyone  
2697 espouse this--the opposite of this proposition, which is  
2698 these need to be neutral, they need to be flexible. There is  
2699 a way to do that. There are established frameworks in  
2700 Federal law that do that.

2701 Mr. {Kennedy.} So if I--just got about a minute left,  
2702 and a discussion that has come up over this legislation a  
2703 couple of times now is over preemption. And so, in your  
2704 mind, and as a practitioner, can you give us some suggestions  
2705 on--does it have to be all or nothing, or are there some ways  
2706 we can present--preempt some things, like the content of the  
2707 notice, for example, but not others, to allow for that  
2708 flexibility?

2709 Ms. {Cable.} Absolutely, yes. Thank you for the  
2710 question. I think preemption absolutely does not need to be  
2711 an all or nothing approach. We have heard the patchwork 47  
2712 or 51 different data notice regimes, approximately 12 data  
2713 security standards. What I hear more, regarding a compliance  
2714 burden, is with responding to a breach, versus how do you  
2715 prevent a breach in the first instance.

2716 I think there is some work that might be done in

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2717 limiting the scope of the preemption to address the specific  
2718 burdens that are being articulated, and enable a rapid  
2719 response to a breach. But I think the states are innovative  
2720 in the field of data security, I think they are nimble. You  
2721 know, our view is the preemption is just simply too broad.

2722 Mr. {Kennedy.} I have only got about 10 seconds left.  
2723 I might submit in writing a question about the--any concerns  
2724 over the enforcement mechanisms, or the limits on the civil  
2725 penalties for your consideration.

2726 Ms. {Cable.} Of course.

2727 Mr. {Kennedy.} Thank you for coming here.

2728 Ms. {Cable.} Happy to answer.

2729 Mr. {Leibowitz.} And if I could just add point to  
2730 respond to your question? I mean, these are--

2731 Mr. {Kennedy.} Yeah.

2732 Mr. {Leibowitz.} It is my--it is on my time, or--

2733 Mr. {Kennedy.} It is not.

2734 Mr. {Leibowitz.} --on your time?

2735 Mr. {Kennedy.} It is up to the Chairman.

2736 Mr. {Leibowitz.} If it is--if the Chairman--

2737 Mr. {Burgess.} Gentleman may respond.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2738 Mr. {Leibowitz.} --unanimous consent? Thank you.

2739 Again, you raise very good questions about how to think

2740 through the next iteration--

2741 Mr. {Kennedy.} Um-hum.

2742 Mr. {Leibowitz.} --and, obviously, we want to work with

2743 you to--

2744 Mr. {Kennedy.} Um-hum.

2745 Mr. {Leibowitz.} --do that.

2746 Mr. {Kennedy.} Okay. Thank you. I appreciate it.

2747 Mr. {Burgess.} Chair thanks the gentleman, gentleman

2748 yields back. Chair recognize the gentlelady from Tennessee,

2749 Ms. Blackburn. Five minutes for questions, please.

2750 Mrs. {Blackburn.} Thank you all, and I appreciate the

2751 conversation, and--that you would be here and weigh in on the

2752 discussion draft. Mr. Leibowitz, I have to say, it looks

2753 normal and natural to see you at that witness table, and we

2754 are happy to have you back.

2755 Ms. Weinman, I want to come to you first. We haven't

2756 talked a lot about the third party notice obligations, so I

2757 would like to have you walk through what you see as the

2758 strengths and weaknesses of the third party notice



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2759 obligations.

2760 Ms. {Weinman.} Thank you for the question. I will  
2761 begin by setting the stage with some defined terms. So the  
2762 covered entity is generally the entity that has the  
2763 relationship with the customer, or the consumer, use  
2764 whichever word you are more comfortable with. And then the  
2765 third party, or another term used in here would be a service  
2766 provider, is the one that might perform services on behalf of  
2767 that covered entity, but would also have personal information  
2768 in their possession as a result of their B to B relationship  
2769 with the covered entity, business to business.

2770 So the gap that I pointed out in my oral statement is  
2771 that it is unclear when the covered entity would be required  
2772 to provide notice to its customers when the third party  
2773 suffered a breach. It is very clear when the covered entity  
2774 would have to provide notice when it itself had been  
2775 breached, but when the third party had been breached, it is  
2776 unclear whether the timeline begins when that third party has  
2777 had the opportunity to determine the scope of its breach, and  
2778 had taken steps to remedying vulnerabilities, and restored  
2779 its systems.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2780 Mrs. {Blackburn.} Okay. Let me ask you something else.  
2781 You mentioned the amount of compliance time, with businesses  
2782 having to comply with all the different state laws. So is  
2783 there any way that you can quantify what this would save to  
2784 businesses by having preemption in place, and having a  
2785 national standard? Have you thought through it in that  
2786 regard, as--the cost savings to business?

2787 Ms. {Weinman.} I don't have a quantifiable number, in  
2788 terms of compliance costs. That is not something that I have  
2789 put together. I can point out, though, in terms of--the  
2790 compliance costs would be considerable, considering the legal  
2791 time. The redirection of resources that could be devoted to  
2792 other critical areas once a data breach occurs is also a  
2793 question of opportunity cost. If you are spending a lot of  
2794 time figuring out your notice regime with 51 different  
2795 frameworks, that is taking time and money away from other  
2796 areas that you can be focusing on--

2797 Mrs. {Blackburn.} Okay.

2798 Ms. {Weinman.} --following a data breach.

2799 Mrs. {Blackburn.} Mr. Duncan, I saw you shaking your  
2800 head. Let me come to you on that, because you mentioned in

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2801 your testimony that you all have for years called on Congress  
2802 to do something on breach notification. You also talk about  
2803 modeling a Federal bill on strong consensus of existing state  
2804 laws, and, in the context of third party notification, all of  
2805 the existing state laws require notice from a third part to a  
2806 covered entity after a breach.

2807 So I want you to talk to me about two things. I want  
2808 you to reconcile your support for a national standard based  
2809 on the state laws with your issues regarding the structure of  
2810 the state laws for the third party. And then also I want you  
2811 to talk a little bit about cost, and the preemption, and what  
2812 it would do to--what it would save consumers and businesses  
2813 in the process.

2814 Mr. {Duncan.} Thank you, Congressman Blackburn. There  
2815 are three very good questions. In terms of the states,  
2816 virtually all of the states do have an arrangement by which  
2817 third parties would report directly to the entity for whom  
2818 they were providing, say, a service, and that would be the  
2819 general rule. What has become increasingly clear to the--to  
2820 a number of state Attorney Generals is that trying to provide  
2821 notice like that in every situation actually will not provide

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2822 effective notice.

2823           There is an example, for example, in our testimony that  
2824 talks about the Hartline breach, which was a huge breach. 80  
2825 million data points, I believe, realized. And in that case,  
2826 Hartline did the right thing. It didn't follow the state  
2827 laws. In fact, it went beyond them, and provided the notice  
2828 itself directly. Had they done otherwise, because Hartline  
2829 was a payment processor for hundreds of retailers, it would  
2830 have had--told each of them, and each of them would have had  
2831 to tell all their customers about Hartline's breach, so  
2832 consumers would have received hundreds of notices for what  
2833 was actually one breach.

2834           So there is becoming a realization among the state AGs  
2835 that we are--really should be focusing on effective notice,  
2836 rather than this strictured--structured notice that is  
2837 contained in some of the state laws. So it is an evolution  
2838 of that. This presents a double problem when we go to the  
2839 subset that Ms. Weinman just talked about, which was service  
2840 providers, because in this case, under the draft language, in  
2841 some circumstances, they would provide no notice at all, and  
2842 that certainly--it shouldn't be a situation that someone who

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2843 knows they have a notice--knows they have a breach can find  
2844 themselves in a situation in which they say nothing to  
2845 anyone, not even to law enforcement.

2846           And finally, as to cost, this is a very significant  
2847 consideration. You must consider that this law is going to  
2848 apply not just to the largest companies in America. It is  
2849 going to apply to the first person who has 15 dry cleaner  
2850 front--shops. How much will he or she have to stay up at  
2851 night, wondering about whether or not they have met an  
2852 amorphous data security standard to--going forward? And that  
2853 imposes tremendous costs on the operation of our businesses.

2854           Mrs. {Blackburn.} Mr. Chairman, my time has expired,  
2855 and I will yield back, but I would ask Mr. Leibowitz, I can  
2856 see that he was trying to respond to that, just to submit in  
2857 writing his response, or someone later can call on him for  
2858 his response to that question.

2859           Mr. {Burgess.} Chair thanks the gentlelady. Gentlelady  
2860 yields back. Recognize Ms. Schakowsky. Five minutes for  
2861 questions, please.

2862           Ms. {Schakowsky.} Thank you, Mr. Chairman. So I  
2863 haven't heard anyone, except for Mr. Leibowitz, say that if

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2864 the bill were to pass as is that consumers would be better  
2865 protected. I didn't hear the first panel or the second  
2866 panel--it seemed to me that lots of people--everyone had  
2867 suggestions of how the bill could be made better. If I am  
2868 wrong, would you tell me that? Okay. So I--and Mr.  
2869 Leibowitz also said he is happy to work with us, so I think  
2870 we have some work to do.

2871 I wanted to ask a question about personal information  
2872 that has come up several times. And--so when--let me ask Ms.  
2873 Cable. In terms of personal information, what does your law  
2874 include? And I want to ask Ms. Moy kind of a more global--  
2875 other states as well. Go ahead, Ms. Cable.

2876 Ms. {Cable.} Thank you for the question. For  
2877 Massachusetts, the definition of personal information is  
2878 actually narrower than what is being considered in this bill.  
2879 It includes name--first name and last name, or first initial  
2880 and last name, plus one of the following components, Social  
2881 Security Number, driver's license number, or other government  
2882 issued ID number, and that is state government issued ID  
2883 number, or a financial account number with or without the  
2884 security code required to access the account.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2885           Ms. {Schakowsky.} So many of us, I think, think that  
2886 the requirement in the bill is too narrow, that it is just  
2887 financial harm. And I would like to get Ms. Moy, if you  
2888 could answer, what kind of information do you think is  
2889 missing now that we are taking this important step of looking  
2890 toward protecting consumers. What do you think ought to be  
2891 there?

2892           Ms. {Moy.} Thank you. Thanks so much for this  
2893 important question. So, as I mentioned in my testimony,  
2894 there are a number of pieces of information that are covered  
2895 by other laws. In particular, health information is covered  
2896 by a lot of states. But I think, you know, we could go back  
2897 and forth about particular pieces of information that should  
2898 or should not be included in the definition of personal  
2899 information here, but the big picture here is really--the  
2900 bottom line is that there are broad categories of personal  
2901 information that are currently covered under a number of  
2902 state laws, and under the--

2903           Ms. {Schakowsky.} Well, let me ask you this, then,  
2904 because I think it would be--help to outline for us. You  
2905 noted that this bill does not protect the serious harms that

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2906 a breach of information could cause, so I am wondering if you  
2907 could draw a picture for us of what some of those serious  
2908 harms could be.

2909 Ms. {Moy.} Sure. So, for example, you could imagine  
2910 that if your e-mail address and password were compromised.  
2911 So that might not be a--an account identifier and a password  
2912 that is necessarily financial in nature, and would fall  
2913 within the scope of this bill, but if my personal e-mails  
2914 were compromised, I am--I would certainly experience some  
2915 harm. I am sure I would experience not only emotional harm,  
2916 but perhaps harm to relationships, perhaps harm to  
2917 reputation. And, you know, and I think that the--a common  
2918 sense question here is just, if my e-mail address and account  
2919 password were compromised, would I want to be notified? And--  
2920 -absolutely. I think that is just there--just some common  
2921 sense there.

2922 Ms. {Schakowsky.} Let me ask you this. Are--let us say  
2923 a woman is a victim of domestic violence--

2924 Ms. {Moy.} Um-hum.

2925 Ms. {Schakowsky.} --but geolocation is not protected.  
2926 Could she be at risk in some way?



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2927           Ms. {Moy.} Right, thank you. So I think one of the  
2928 things that I did highlight in my written testimony is that  
2929 because both of--the definition of personal information, and  
2930 the harm trigger that is premised on financial harm, there  
2931 are categories of information, like geolocation information,  
2932 or like information about call records, that, if compromised,  
2933 could result in physical harm. So a domestic violence  
2934 victim, for example, might be concerned not only about her  
2935 geolocation information, but perhaps about her call records.  
2936 If she called a hotline for victim assistance, or if she  
2937 called a lawyer, those are pieces of information that she  
2938 absolutely would not want to be compromised.

2939           Ms. {Schakowsky.} In terms of the role of the FTC  
2940 having some flexibility in defining what personal information  
2941 would be, what position have you taken?

2942           Ms. {Moy.} Right. So I think it is--I think that it is  
2943 critical that we provide for flexibility in the definition of  
2944 personal information in one way or another. Whether it is  
2945 through agency rulemaking, or through state law, it is really  
2946 important that we be able to adapt a standard to changing  
2947 technology, and changing threats.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2948           So I mentioned in my testimony the growing trend of  
2949 states including medical information in their definition of  
2950 personal information. In fact, two states just this year  
2951 have passed bills that will include that information in their  
2952 breach notification later this year, and that is not an  
2953 arbitrary change. The reason that that is changing is  
2954 because there is a growing threat of medical identity theft,  
2955 and it is really important to build in flexibility to account  
2956 for those changes.

2957           Mr. {Leibowitz.} And if I could just follow up on Ms.  
2958 Moy's points very quickly, in support, I think, of most of  
2959 them. You know, I think geolocation--and your point. I  
2960 think geolocation is critically important. When we were at  
2961 the FTC, we expanded geolocation under COPPA to be a  
2962 condition present. It is something you may want to take a  
2963 look at.

2964           It is also important to note that the Massachusetts law,  
2965 which is one of the most progressive laws of the state, has a  
2966 narrower definition of data security. This is a well-  
2967 intentioned piece of legislation, and reasonably we can  
2968 disagree about where to draw the line, but it is broader than

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2969 38 states, that don't have it.

2970           And then the point--I--the other two very quick points I  
2971 want to make, on the ISP point that you mentioned before,  
2972 Mallory--Mr. Duncan, you know, if a service--aware of a data  
2973 security breach, they must notify the company of the breach,  
2974 and they have an obligation to reasonably identify any  
2975 company, to try to reasonably identify.

2976           And then, finally, on rulemaking, obviously, I came from  
2977 the FTC, I came and testified in support of this legislation,  
2978 or signed testimony. I would just say, and maybe this is  
2979 overall for the legislation, this is my belief in it, it  
2980 always was when I was there, is you just don't want to let  
2981 the perfect be the enemy of the good here. You want to make  
2982 sure you move forward for consumers. Reasonable people can  
2983 disagree about exactly where that is, but getting some things  
2984 sometimes is better than, you know, not getting everything.

2985           Mr. {Burgess.} The Chair thanks the gentleman for his  
2986 observations. Gentlelady's time has expired. Chair  
2987 recognizes the gentlelady from Indiana, Ms. Brooks. Five  
2988 minutes for questions, please.

2989           Mrs. {Brooks.} Thank you, Mr. Chairman, and I want to

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

2990 build on what the gentleman from Massachusetts was saying, is  
2991 that we have to get this right, and--perfect is the enemy of  
2992 good here. And I have heard--I am not familiar with  
2993 Massachusetts statute, and, obviously, with there being so  
2994 many statutes, the problem is that we in Congress, while we  
2995 have been talking about it for years and years and years, and  
2996 I applaud all the work that has been done in Congress in the  
2997 past, we have got to move something forward here, because  
2998 terrorist organizations, nation-state organizations, are  
2999 continue--they are going to always continue to come up with  
3000 more ways and new ways to hack and get this information.

3001         And it is becoming, I think, one of our constituents'  
3002 greatest security concerns, truly, and we have got to get  
3003 this right. And I don't believe that having 51 different  
3004 standards is good. We have got to get, you know, we have got  
3005 to move on this and improve. And I think--my previous  
3006 question to the director of the FTC, the reasonable security  
3007 practice, and if we were to adopt, for instance,  
3008 Massachusetts, how you have set out, and what I would love to  
3009 see is the state Attorney Generals work with the Committee  
3010 and the members who have put forth this legislation, and let

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3011 us get this right.

3012           And so if--for instance, if the reasonable security  
3013 practices that you delineate in Massachusetts, those are  
3014 flexible, but yet they set out the process, would that  
3015 satisfy you on the reasonable security piece, Ms. Cable?

3016           Ms. {Cable.} Yes, thank you for the question, and I  
3017 agree and appreciate this is a critical issue, and action--  
3018 there needs to be action, and I really applaud the  
3019 Subcommittee for taking up this issue, because it is  
3020 complicated and it is difficult.

3021           I think, you know, I happen to very much like the  
3022 Massachusetts data security regulations, but, of course, I  
3023 have to say that.

3024           Mrs. {Brooks.} Sure.

3025           Ms. {Cable.} I think they are, however, a good  
3026 framework, a recognized framework, and something that  
3027 commercial entities are used to seeing. And I think the  
3028 issue with preemption, what makes it concerning to us, is the  
3029 standard of data security that is being set. We don't think  
3030 it is sufficiently defined, and therefore we think, as a  
3031 result, it may not be sufficiently robust. And so, at least

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3032 from Massachusetts perspective, this is not better off for  
3033 our consumers if reasonable security measures and practices  
3034 result in a downward harmonization across the nation of a  
3035 lower standard of security.

3036 And I might add, lower security, logically, I think,  
3037 will result in an increased incidence of breaches, an  
3038 increase in notice obligation, and an increase of all of the  
3039 problems we are discussing today. I really think the data  
3040 security standard is a critical element. I think the  
3041 reasonableness standard is maybe a good lode star guidepost,  
3042 but this--the measures and practices need to be more defined.

3043 Mrs. {Brooks.} Mr. Leibowitz, would you like to comment  
3044 on those remarks?

3045 Mr. {Leibowitz.} Well, I mean, at 50,000 feet I agree  
3046 that you don't want to ratchet down, you want to ratchet up  
3047 the level of data security. I think the fact that 38 states  
3048 don't have any data security obligations at all is very  
3049 telling. And, again, as Ms. Cable acknowledged, you know,  
3050 one of the most progressive pieces of legislation that states  
3051 have written is the Massachusetts law. On the data security  
3052 side, it has a narrower definition.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3053           So I think, again, and going back to Mr. Welch's point  
3054 and Mr. Cardenas's point, it is like what do people care  
3055 about when--what hackers care about, they care about the  
3056 personal identification and the financial information. And  
3057 what do consumers care about, and at the FTC--and the FTC  
3058 continues to do great work here, you know, they care about  
3059 their Social Security Number. They care about their  
3060 financial information being taken. They care about, you  
3061 know, economic harm more than anything else. And that is  
3062 what drives this problem more than anything else. It is not  
3063 ideological groups. It is, you know, people engaged in fraud  
3064 and criminal activities that the FTC and the state AGs have  
3065 been prosecuting, will continue to be able to do in the bill.

3066           Mrs. {Brooks.} Thank you. And one completely different  
3067 issue, Ms. Weinman, you talked about the providers must  
3068 restore their system, that entities should restore their  
3069 system before notification. Can you explain why that would  
3070 be necessary when it does seem that speed in getting out  
3071 notifications--although we know that often those who are  
3072 breaching and hacking can sit on this information for years,  
3073 they don't often use it immediately. But why do you propose

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3074 that an entity needs to have the time to restore its system,  
3075 as you have said, before notification?

3076 Ms. {Weinman.} As currently drafted, the bill does  
3077 allow that restoration of system on--for a covered entity,  
3078 and I think it is critical that that be the case because if  
3079 an entity provides notification, it is essentially making  
3080 public that its system has been compromised, and it could  
3081 render itself further vulnerable to additional attacks by  
3082 those same hackers, or other hackers. So I thank, and  
3083 applaud, the Subcommittee for recognizing that point in time  
3084 when notification should begin should be at a time when the  
3085 system has been restored.

3086 Mrs. {Brooks.} Thank you. I yield back.

3087 Mr. {Burgess.} The Chair thanks the gentlelady, and  
3088 Chair recognizes gentleman from Vermont, Mr. Welch for 5  
3089 minutes for questions.

3090 Mr. {Welch.} Thank you very much, sir. I want to take  
3091 up a bit from where my colleague, Ms. Brooks, was with the  
3092 Attorney General's Office from Massachusetts. First of all,  
3093 thank you for your testimony. Second, thanks for the good  
3094 work that Massachusetts does. Third, we are pretty proud of



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3095 our Attorney General and consumer protection in Vermont.  
3096 They have a standard and an--they have a solid standard, and  
3097 an aggressive consumer protection division, like you do, and  
3098 they have made some of the same arguments to me about this  
3099 bill that you just made, so message received.

3100 But I just wanted to go through a few things. Number  
3101 one, the bill does use this term reasonableness, and I think  
3102 there has been a debate, even--not--on all sides, including  
3103 among consumer activists, whether something that is flexible  
3104 has the potential to meet the challenges as they emerge, as  
3105 opposed to--what I heard in your testimony is a more detailed  
3106 set of guidelines that is--according to your testimony is  
3107 working for you.

3108 But I guess I am just looking for some acknowledgment  
3109 that there is a legitimate argument to approach it in a  
3110 prescriptive way, or in a general way that gives a little  
3111 more flexibility to the enforcer, in this case Massachusetts.  
3112 Would you agree with that?

3113 Ms. {Cable.} Yes, thank you for your question, and I  
3114 would reiterate I work closely with colleagues from the  
3115 Vermont Attorney General's Office. It is a fantastic office,

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3116 and I enjoy working with them. I think the issue of data  
3117 security standards, and whether they are flexible--

3118 Mr. {Welch.} Right.

3119 Ms. {Cable.} --flexible or prescriptive, I think you  
3120 can have standards that articulate components of what a data  
3121 security system framework should look like, but an awful lot  
3122 of flexibility with how you meet those standards, and I--

3123 Mr. {Welch.} Well, right, and that is where it is  
3124 genuinely difficult. Because, you know, if Ms. Brooks was  
3125 able to get all the Attorney Generals to come up with what  
3126 was the best approach, that might be persuasive to all of us,  
3127 because there are Republican and Democratic Attorney Generals  
3128 out there.

3129 A second thing that I wanted to talk about is this  
3130 question of an obligation on the part of the companies.  
3131 There is an enormous incentive for thieves, criminals, to try  
3132 to hack our information. They get our money. There is an  
3133 enormous incentive--I am looking for all you--your reaction  
3134 on this--for companies to have their computer systems be as  
3135 safe as possible, because they are victims too in this case.  
3136 I mean, look what happened at Target. People lose their

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3137 jobs. It is brutal on the bottom line for these companies.

3138 So I see that as a practical reality that we can take

3139 advantage of. I mean, is that consistent with you, as an

3140 enforcer?

3141 Ms. {Cable.} I would absolutely agree, and I would

3142 note, you know, much of my effort is not spent trying to find

3143 gotcha moments and--

3144 Mr. {Welch.} Right.

3145 Ms. {Cable.} --enforcing. We have received notice of

3146 over 8,600--

3147 Mr. {Welch.} Yeah.

3148 Ms. {Cable.} --breaches, and I think, we ran the

3149 numbers, we have had 13 actions.

3150 Mr. {Welch.} But you would be in agreement--

3151 Ms. {Cable.} I would, and I would--

3152 Mr. {Welch.} Yeah.

3153 Ms. {Cable.} Most of my time is spent--

3154 Mr. {Welch.} I don't have much time, so let me get a--

3155 Ms. {Cable.} Of course. I apologize.

3156 Mr. {Welch.} --few more. You have been very helpful.

3157 The other thing Mr. Duncan was talking about, effective

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3158 notice, and this goes back, again, to kind of practicality.  
3159 If I get these bank notices when I do this mortgage  
3160 refinancing, it literally gives me a headache, and I get less  
3161 information. All I need to know are three things, what is my  
3162 rate--what is my interest rate, when is the payment due, and  
3163 what is the penalty if I don't meet the time? That is all I  
3164 need to know. And--so this effective notice issue, I think,  
3165 is something that, on a practical level, all of us want to  
3166 take into account.

3167         So let me go, Ms. Moy, to you. I want to, first of all,  
3168 thank you and your organization for the great work you have  
3169 done, and also for being available to try to answer my  
3170 questions.

3171         Ms. {Moy.} Thank you.

3172         Mr. {Welch.} You had mentioned something that every  
3173 single one of us would be really concerned about, if there  
3174 was any way that we were passing legislation that was going  
3175 to make a woman of domestic violence more vulnerable. All of  
3176 us would be against that, okay? So I don't see in this  
3177 legislation how that is happening, but if, in your view, it  
3178 is, I would really welcome a chapter and verse specification

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3179 as to what we would have to do to make sure that didn't  
3180 happen. And I think we would all want to be on board on  
3181 that. So could you help us with that--

3182 Ms. {Moy.} Thank you, I appreciate that question, and I  
3183 have appreciated working with your office as well. So I  
3184 think, you know, this is--this question mostly gets to what  
3185 the--what standard is set for the harm trigger, right? I  
3186 mean, because there are certain types of information, or  
3187 certain situations where information may be compromised or  
3188 accessed in an unauthorized manner, and you could look at  
3189 that situation and say, this information really couldn't be  
3190 used for financial harm, or we think it is unlikely that that  
3191 is the--that was the motivation of the person who accessed  
3192 that information.

3193 Mr. {Welch.} Okay. My time is running up, so I--

3194 Ms. {Moy.} Yes.

3195 Mr. {Welch.} --apologize for interrupting, but if--

3196 Ms. {Moy.} Um-hum.

3197 Mr. {Welch.} --you sent us a memo on that, and--

3198 Ms. {Moy.} Absolutely.

3199 Mr. {Welch.} --Attorney Cable, if you sent us some

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3200 specifics, I--that would be helpful to the Committee, because  
3201 I know Ms. Schakowsky was very interested in a lot of the  
3202 points you made, as well as all of us, I think.

3203 Ms. {Moy.} Absolutely.

3204 Mr. {Welch.} Thank you.

3205 Ms. {Moy.} Thank you.

3206 Mr. {Welch.} I yield back.

3207 Mr. {Burgess.} Chair thanks the gentleman. Chair  
3208 recognizes the Vice Chair of full--of the Subcommittee, Mr.  
3209 Lance. Five minutes for questions, please.

3210 Mr. {Lance.} Thank you very much, Mr. Chairman.

3211 Mr. Leibowitz, in your opinion, what benefit have class  
3212 actions brought to consumers after a data breach?

3213 Mr. {Leibowitz.} Well, let me start by saying, I think  
3214 class actions have an enormous value in a lot of areas.  
3215 Civil rights areas, others as well. In this area, I don't  
3216 think that class actions have much benefit, except for the  
3217 lawyers who bring them. And what they also do is they  
3218 incentivize, or the create incentives, I think, for companies  
3219 to emphasize legal protections, rather than actual reasonable  
3220 data security.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3221           And I will just make sort of one other point, which goes  
3222 back to the FTC, which is, if the FTC brings a case, and it  
3223 gets compensation for consumers, all that compensation goes  
3224 back to the consumers. They--\$200 million to 400,000 people  
3225 who were victims of mortgage service fraud by Countrywide,  
3226 and that is one other benefit. But I also believe that, you  
3227 know, class actions can be vitally important, as I am sure  
3228 you do, in some areas.

3229           Mr. {Lance.} In other words, your point is that when  
3230 the FTC does it, the--FTC personnel are in the public sector,  
3231 and the full benefit goes to those--

3232           Mr. {Leibowitz.} The entire--

3233           Mr. {Lance.} --who have been harmed?

3234           Mr. {Leibowitz.} Yes.

3235           Mr. {Lance.} It is an indication why we should be  
3236 supportive of our Federal workforce--

3237           Mr. {Leibowitz.} And--

3238           Mr. {Lance.} --and for colleagues who serve in Federal  
3239 service. Would others like to comment on that? Attorney  
3240 General Cable?

3241           Ms. {Cable.} If I may?

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3242 Mr. {Lance.} Certainly.

3243 Ms. {Cable.} Thank you, Congressman.

3244 Mr. {Lance.} Certainly.

3245 Ms. {Cable.} I would just note--consumer restitution is  
3246 a critical tool that we have in our toolbox under our  
3247 Consumer Protection Act. We use it--we like to use it. If  
3248 we can get the money, we distribute it. I noted under this  
3249 version of this bill, it does not expressly allow us to seek  
3250 consumer restitution, and it also denies the consumer a  
3251 private right of action. We think that is a bit of an  
3252 oversight in the event a consumer is actively harmed here.  
3253 State AGs under this bill would not be able to seek consumer  
3254 restitution, under one interpretation.

3255 Mr. {Lance.} Thank you, Attorney General. Mr.  
3256 Leibowitz, do you wish to comment further or not? No? Thank  
3257 you.

3258 Mr. {Leibowitz.} No, sir.

3259 Mr. {Lance.} Ms. Weinman, do you have a concern about  
3260 state common law claims adding additional security or  
3261 notification requirements for companies if a Federal law is  
3262 enacted?



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3263           Ms. {Weinman.} I think that this bill strikes a useful  
3264 balance in pre-empting the current state data security  
3265 requirements and the breach notification, so I think this  
3266 bill strikes a good balance in that area.

3267           Mr. {Lance.} And you believe that because the country  
3268 would move forward uniformly, and this would be something  
3269 that would be on the books for the entire nation?

3270           Ms. {Weinman.} Yeah, and it would streamline the  
3271 notification process across the board, across the 51 regimes  
3272 for which I have, you know, a 19 page chart. So I think that  
3273 would definitely be useful.

3274           Mr. {Lance.} Yes. Thank you. Mr. Chairman, I yield  
3275 back the balance of my time.

3276           Mr. {Burgess.} Chair thanks the gentleman. Chair  
3277 recognizes the gentleman from New Jersey, Mr. Pallone. 5  
3278 minutes for questions, please.

3279           Mr. {Pallone.} Thank you, and I have been to, like,  
3280 three different meetings since I was last here, so hopefully  
3281 I will be understandable here. Under current law the FTC  
3282 does not have enforcement authority over common carriers,  
3283 including telecommunications, cable, and satellite services,

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3284 and the discussion draft lifts the common carrier exception  
3285 to allow the FTC to bring enforcement actions for violations  
3286 of the provisions of this bill.

3287           And I wanted to ask each member of the panel, and I am  
3288 just looking for a yes or no because I have a whole series of  
3289 things here, if you could just say yes or no, assuming the  
3290 draft did not include preemption of the Communications Act in  
3291 Section 6C, do you support lifting the common carrier  
3292 exceptions in the context of data security and breach  
3293 notifications, yes or no? We will start to the left.

3294           Mr. {Leibowitz.} Yes.

3295           Mr. {Pallone.} Ms. Cable?

3296           Ms. {Cable.} I have--I apologize, I think I am out of  
3297 my expertise, so--

3298           Mr. {Pallone.} You have no response?

3299           Ms. {Cable.} I have no response.

3300           Mr. {Pallone.} All right. Mr. Duncan?

3301           Mr. {Duncan.} We don't have a preference as to which  
3302 agency covers it.

3303           Mr. {Pallone.} That is--

3304           Mr. {Duncan.} The only requirement is that everyone be

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3305 covered.

3306 Mr. {Pallone.} Okay. Ms. Moy, yes, no?

3307 Ms. {Moy.} If it did not eliminate provisions of the  
3308 Communications Act, yes.

3309 Mr. {Pallone.} Okay. And our last--

3310 Ms. {Weinman.} I will give a similar response to Mr.  
3311 Duncan, that it is not an issue that would implicate ITI  
3312 members, so--

3313 Mr. {Pallone.} All right.

3314 Ms. {Weinman.} --I am not expressing a preference one  
3315 way or the other.

3316 Mr. {Pallone.} All right. Now I just want to ask my  
3317 next two questions of Ms. Moy, because I may not have a lot  
3318 of time. Lifting the common--I have two. First, lifting the  
3319 common carrier exception without nullifying the data security  
3320 and breach notification provisions of the Communications Act  
3321 would mean that there are two cops on the beat, so to speak,  
3322 so what are the benefits to joint jurisdiction among the FCC  
3323 and the FTC? To Ms. Moy only.

3324 Ms. {Moy.} Thank you, thank you so much. So I think  
3325 one of the major benefits is that the two agencies have

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3326 different strengths, and they could work together to use  
3327 their strengths to complement each other and ensure the best  
3328 protection for consumers. For example, the FCC is primarily  
3329 a rulemaking agency that uses its authority to set standards  
3330 prospectively, and the FTC is primarily an enforcement  
3331 authority. It would be really nice if they could work  
3332 together to establish the standards in the first place, and  
3333 then enforce them in the second place.

3334 I think also the FCC has a lot of very important  
3335 expertise in this area, working with telecommunications  
3336 networks, and other communications networks, and just--and  
3337 the focus on privacy is a little bit different. The focus on  
3338 privacy at the FCC is more about the reliability of the  
3339 networks, and the fact that consumers have no choice but to  
3340 share information with these very important networks in their  
3341 lives, whereas the focus of the FTC on privacy is a little  
3342 bit more about what is fair with respect to consumers. And,  
3343 again, it would just be really nice if those agencies could  
3344 work together in that area to use their expertise, or their  
3345 respective expertise, in a complementary manner.

3346 Mr. {Pallone.} And then I have a second one to you

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3347 only, and if I have time, we are going to go to the others.  
3348 Do you think there are any drawbacks to having FTC and FCC  
3349 enforcement? Are you concerned about consumers being  
3350 confused by having two enforcing agencies?

3351 Ms. {Moy.} I am not concerned about that. I think that  
3352 where we have seen agencies work together in the past, I  
3353 don't think that there really is confusion for consumers.  
3354 For example--I am sorry, I am blanking, but the FTC and the  
3355 FCC have worked together on the, for example, Do Not Call,  
3356 and--of telecommunications customers. And I really don't  
3357 think that there is any risk of confusion for consumers of  
3358 having those agencies work together.

3359 Mr. {Pallone.} All right, one more question. I will  
3360 start with you, and then--we have time, we will go to the  
3361 others. Do you have any suggestions for how legislation can  
3362 ensure that companies are not burdened by duplicative  
3363 enforcement?

3364 Ms. {Moy.} I am sorry, that companies are not burdened  
3365 by--

3366 Mr. {Pallone.} By duplicative enforcement. Any  
3367 suggestions for how legislation could ensure that companies

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3368 are not burdened by duplicative enforcement?

3369 Ms. {Moy.} Well, I think that--I mean, the premise of  
3370 the question is that duplicative enforcement is necessarily  
3371 more burdensome for companies, and I don't think that that is  
3372 necessarily the case. You know, as I said, the FCC and the  
3373 FTC can work together and use--and--to formulate standards  
3374 and enforce them in a uniform way. And I think that they  
3375 would have an incentive to do that, so as not to--so as to  
3376 maximize the efficiency of their resources toward that goal.  
3377 And I think that that incentive would sync up quite nicely  
3378 with the incentive of companies--of having the two agencies  
3379 work in step with each other, so as not to seem like two  
3380 separate--totally separate regimes.

3381 Mr. {Pallone.} All right, thanks. I think I have run  
3382 out of time, Mr. Chair.

3383 Mr. {Duncan.} If I--

3384 Mr. {Pallone.} Thank you.

3385 Mr. {Duncan.} If I might just mention, on that point,  
3386 under the structure of the bill, both the FTC and the state  
3387 AGs would have enforcement authority, and that is an option  
3388 that works, at least in that context. From our perspective,

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3389 as long as everyone has the same obligations, and duties, and  
3390 responsibilities, then it is less of an issue.

3391 Mr. {Leibowitz.} Yeah. And the only thing I would add  
3392 is that there is a--sort of an evolving consensus that what  
3393 you really want, Mr. Pallone, is a flexible enforcement  
3394 standard that is strong with enforcement. And you also want  
3395 to treat the same information the same way, not under  
3396 different regimes. So, you know, Google can collect  
3397 information, Verizon can collect information, Comcast can  
3398 collect information. A variety of other companies can.

3399 And, for the most part, I think where this bill wants to  
3400 go is in a data breach context. And in the data security  
3401 context, more importantly, treat them equally.

3402 Mr. {Burgess.} Chair thanks the gentleman. Gentleman's  
3403 time has expired. Chair recognizes Mr. McNerney. Five  
3404 minutes for your questions, please.

3405 Mr. {McNerney.} Well, I want to thank the Chairman and  
3406 the Ranking Member for allowing me to participate in this  
3407 hearing, even though I am not a member of the Subcommittee.  
3408 I appreciate that. And I want to say I appreciate the  
3409 efforts of my colleagues, Mr. Welch, Mr. Burgess, and Mr.--

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3410 Mrs. Blackburn for crafting this bill. It is clearly needed.  
3411 And it may not be perfect yet, but it can be improved, and it  
3412 is much better to start from the draft than to start over--  
3413 than to over to start over. So I have a couple of questions  
3414 here.

3415 Ms. Weinman, you mentioned that the civil penalties for  
3416 breach of notification are excessive for a company that is a  
3417 victim of a criminal act. Do you think it would be okay to  
3418 lower the penalties, or to have some flexibility? And if you  
3419 think flexibility is the way to go, how can you do that in  
3420 this kind of a bill?

3421 Ms. {Weinman.} I think lowering would be a good step,  
3422 and I think there is flexibility built into the assessment of  
3423 civil penalties within the bill, but I think lower the  
3424 maximum penalties would make sense in the context of the fact  
3425 that companies themselves are the victims of criminal  
3426 hackers. So there is some discretion with regard to civil  
3427 penalties within the bill, however I do think the maximum  
3428 amounts set out in there should be lower. And I note that  
3429 the current figures in there are, in fact, five times higher  
3430 than what we have previously seen in other proposals, so I



**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3431 just make a note of that.

3432 Mr. {McNerney.} Well, I mean, you could consider some  
3433 breaches to be gross negligence, and deserving of significant  
3434 penalties, so--

3435 Ms. {Weinman.} Well, that flexibility is built into the  
3436 language, but I do think that the ceiling could be lower in  
3437 the draft.

3438 Mr. {McNerney.} Thank you. Ms. Moy, you know,  
3439 preemption is a very tricky issue. We want states to have  
3440 flexibility, but you mention that there ought to be a floor.  
3441 But how could you create legislation that had a floor, but  
3442 allowed states like Massachusetts flexibility to go, you  
3443 know, more stringent, if they wanted?

3444 Ms. {Moy.} I think--thank you for the question, and  
3445 thank you. I do recognize that it is very difficult to craft  
3446 the appropriate standard here, and thank you for taking up  
3447 this difficult issue. I, you know, I think that you could  
3448 set a standard that says, this is the minimum standard, and  
3449 that state laws will not be preempted to the extent that they  
3450 create additional standards above that, or beyond that.

3451 But, you know, but also, as I have said in the written

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3452 testimony, and as I mentioned earlier, we are not necessarily  
3453 opposed to the idea of preemptive legislation, but I do think  
3454 that it is important, if we are going to do that, to ensure  
3455 that the new Federal standard, the new uniform Federal  
3456 standard, is better for consumers than the current draft. I  
3457 just--I think it is really important to strike the proper  
3458 balance between preemption and protections for consumers, and  
3459 this just doesn't quite get us there.

3460 Mr. {McNerney.} Now, you mentioned that you felt that  
3461 the draft would lower consumer protections over a wide range  
3462 of consumer protections. Could the bill be strengthened to  
3463 include those current protections?

3464 Ms. {Moy.} I believe that it could be, and I think--I  
3465 would be very happy to work with the Subcommittee to figure  
3466 out ways that we could get there.

3467 Mr. {Duncan.} Congressman--

3468 Mr. {McNerney.} Thank you.

3469 Mr. {Duncan.} --one of the reasons that we are here  
3470 today is because there are already 51 conflicting laws out  
3471 there. If Congress doesn't simplify the system to some  
3472 extent, then we will simply have 52 laws out there, and that

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3473 is not moving us forward.

3474 Mr. {McNerney.} Thank you. Well, Mr. Duncan, you  
3475 mentioned that--the importance of enacting laws that holds  
3476 accountable all entities that handle personal information.  
3477 Can you discuss how you would improve the draft legislation  
3478 to modify the covered entities?

3479 Mr. {Duncan.} Certainly. We would expect that a good  
3480 law would require that every covered entity have the same  
3481 obligation, that third parties--for example, the way the bill  
3482 is written now, some entities do not even have a duty to  
3483 determine--to examine and determine whether or not they can  
3484 find information out about a breach. There has got to be the  
3485 same level requirement all the way across the board.

3486 Congresswoman Schakowsky asked earlier whether or not we  
3487 could support this legislation. I would say this draft is a  
3488 major improvement over what we have seen before, but if we  
3489 could have equal applicability across all entities, and fix  
3490 some of the issues with the FTC, we could support this.

3491 Mr. {McNerney.} Thank you--a lot of good information  
3492 has come out that might help improve the bill, so, Mr.  
3493 Chairman, I yield back. Thank you again.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3494 Mr. {Burgess.} Chair thanks the gentleman. Gentleman  
3495 does yield back. The Chair recognizes Mr. Pallone of New  
3496 Jersey for a unanimous consent request.

3497 Mr. {Pallone.} Thank you, Mr. Chairman. I ask  
3498 unanimous consent to submit for the record a letter from 12  
3499 consumer groups to yourself and Ms. Schakowsky.

3500 Mr. {Burgess.} Without objection, so ordered.

3501 Mr. {Pallone.} I guess we have another one too, Mr.  
3502 Chairman, from the Consumers' Union, in addition to the one  
3503 from everyone else.

3504 Mr. {Burgess.} The Chair thanks the gentleman. Without  
3505 objection, so ordered.

3506 [The information follows:]

3507 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

3508           Mr. {Burgess.} Seeing that there are no further members  
3509 seeking to ask questions, I do want to thank all of our  
3510 witnesses. I know this has been a long hearing, but I thank  
3511 you for participation today.

3512           Before we conclude, I would like to include the  
3513 following documents to be submitted for the record by  
3514 unanimous consent. A letter on behalf of the National--of  
3515 the Credit Union National Association, a letter on behalf of  
3516 the Marketing Research Association, a letter on behalf of the  
3517 National Association of Federal Credit Unions, a letter on  
3518 behalf of the Online Trust Alliance, a letter on behalf of  
3519 the Consumers' Union, statement on behalf of the National  
3520 Association of Convenience Stores, a letter on behalf of the  
3521 American Bankers' Association, the Clearing House, Bankers'  
3522 Consumer Association, Credit Union National Association,  
3523 Financial Services Roundtable, Independent Community Bankers  
3524 of America, and the National Association of Federal Credit  
3525 Unions, and the response of the Secret Service to questions  
3526 submitted for the record at our previous Subcommittee data  
3527 breach hearing on January 27, 2015.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

3528 [The information follows:]

3529 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

|

3530           Mr. {Burgess.} Pursuant to Committee rules, I remind  
3531 members they have 10 business days to submit additional  
3532 questions for the record, and I ask witnesses to submit their  
3533 response within 10 business days upon receipt of the  
3534 questions. I thank everyone for their participation this  
3535 morning. This Subcommittee hearing is adjourned.

3536           [Whereupon, at 1:15 p.m., the Subcommittee was  
3537 adjourned.]