

**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 BURDETTE

3 HIF027.170

4 WHAT ARE THE ELEMENTS OF SOUND DATA BREACH LEGISLATION?

5 TUESDAY, JANUARY 27, 2015

6 House of Representatives,

7 Subcommittee on Commerce, Manufacturing, and Trade

8 Committee on Energy and Commerce

9 Washington, D.C.

10 The subcommittee met, pursuant to call, at 11:01 a.m.,

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

12 Michael Burgess [Chairman of the Subcommittee] presiding.

13 Members present: Representatives Burgess, Lance,

14 Blackburn, Harper, Guthrie, Olson, Kinzinger, Bilirakis,

15 Mullin, Upton (ex officio), Schakowsky, Clarke, Kennedy,

16 Cardenas, Rush, Butterfield, Welch, and Pallone (ex officio).

**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           Staff present: Charlotte Baker, Deputy Communications  
18 Director; Leighton Brown, Press Assistant; Graham Dufault,  
19 Counsel, Commerce, Manufacturing, and Trade; Melissa  
20 Froelich, Counsel, Commerce, Manufacturing, and Trade; Kirby  
21 Howard, Legislative Clerk; Paul Nagle, Chief Counsel,  
22 Commerce, Manufacturing, and Trade; and Olivia Trusty,  
23 Counsel, Commerce, Manufacturing, and Trade; Michelle Ash,  
24 Democratic Counsel, Commerce, Manufacturing, and Trade; Jeff  
25 Carroll, Democratic Staff Director; Lisa Goldman, Democratic  
26 Counsel, Commerce, Manufacturing, and Trade; Tiffany  
27 Guarascio, Democratic Deputy Staff Director; and Ashley  
28 Jones, Democratic Director of Outreach and Member 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.**

|  
29           Mr. {Burgess.} Well, good morning, everyone. Before we  
30 begin our first subcommittee meeting of the 114th Congress,  
31 the ranking member and I would like to briefly recognize new  
32 members of the subcommittee. For the benefit of the ranking  
33 member, I am not a new member. I was on this subcommittee  
34 several terms ago. So I am back on the subcommittee. For  
35 that I am grateful, but on the majority side--I don't believe  
36 she has joined us yet. We have Ms. Brooks representing the  
37 5th District of Indiana and Mr. Markwayne Mullin representing  
38 Oklahoma's 2nd District. Welcome to the committee, welcome  
39 to the subcommittee. We are grateful and excited to have you  
40 on board. For the minority, subcommittee Ranking Member  
41 Schakowsky will introduce her new members.

42           Ms. {Schakowsky.} Thank you, Mr. Chairman, for just  
43 letting me say how much I look forward to working with you on  
44 this subcommittee. New members include Yvette Clarke. She  
45 represents New York's 9th Congressional District as a proud  
46 Brooklyn native with strong roots planted in her Jamaican  
47 heritage. She is an outspoken advocate for district, always  
48 working to champion the middle class and those who aspire 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.**

49 reach it. Her district has become a center of innovation for  
50 healthcare and includes some of the best hospitals, trade  
51 associations, and businesses in the industry. I look forward  
52 to her bringing her tenacity, deep knowledge, and enthusiasm  
53 to this subcommittee.

54 Next to her is Joe Kennedy who serves the people of  
55 Massachusetts' 4th, has dedicated his life to public service,  
56 and brings with him a firm commitment to social justice and  
57 economic opportunity. Joe has previously served in the Peace  
58 Corps, worked as an International Development Analyst for the  
59 United Nations' Millennium Project, and as an anti-poverty  
60 consultant abroad. I know that he will bring that passion  
61 for public service and economic growth to everything he does  
62 on the subcommittee. And not here now but also a new member  
63 of the subcommittee is Tony Cardenas representing  
64 California's 29th Congressional District. He has made a name  
65 for himself by always advocating strongly on behalf of his  
66 constituents on issues like juvenile justice, immigration,  
67 higher education, and economic improvement. He has brought  
68 hard work and dedication to his 16 years of public service on  
69 behalf of the people of the Northeast San Fernando Valley.

**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.**

70 As a former small business owner, an engineer, head of the  
71 California Budget Committee, and as a leader in environmental  
72 progress in the City of Los Angeles, I am certain Tony will  
73 be able to lead his expertise to our subcommittee's progress.  
74 Thank you, Mr. Chairman.

75 Mr. {Burgess.} Thank you, Ranking Member Schakowsky.  
76 We welcome all members of the subcommittee back and look  
77 forward to working with each and every one of you in the  
78 114th Congress.

79 Before I get started, I also want to recognize a  
80 visiting delegation of the legislative staff from the  
81 Parliaments of Georgia, Kosovo, Macedonia, and Nepal through  
82 the House Democracy Partnership. They are in town for a  
83 seminar on strengthening committee operations and are  
84 observing today's hearing as part of the program. I hope  
85 they are able to learn a great deal, both today and during  
86 their tenure here the rest of the week.

87 Ms. {Schakowsky.} Mr. Chairman, could they acknowledge  
88 themselves so we can all see who they are. Great. Thank  
89 you.

90 Mr. {Burgess.} Welcome. Thank you for coming. I am

**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.**

91 glad you were able to make it here with the weather.

92 The Subcommittee on Commerce, Manufacturing, and Trade  
93 will now come to order. I will recognize myself for 5  
94 minutes for the purposes of an opening statement.

95 The purpose of today's hearing is to move one step  
96 closer to a single, federal standard on data security and  
97 breach notification. Increasingly, our personal details,  
98 which we need to verify financial transactions, are converted  
99 into data and uploaded to networks of servers, and not always  
100 can those servers be protected with a simple lock and key.  
101 We benefit immensely from the quick access and command this  
102 system gives us. Global commerce is literally at our  
103 fingertips on a daily basis.

104 And yet such a dynamic environment brings with it  
105 dynamic, evolving risks. As our options multiply, so must  
106 our defensive measures. Those defensive measures must adapt  
107 quickly. As several commentators have noted in testimony  
108 before this subcommittee, it is no longer a matter of if a  
109 breach occurs. It is when and what happens when.

110 Even so, questions remain as to whether businesses are  
111 doing enough to prevent security breaches. That is why 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.**

112 believe federal legislation should include a single but  
113 flexible data security requirement. Now, about 12 states  
114 have already implemented such a requirement on commercial  
115 actors that are not banks or health care providers.

116       A single requirement across the states would give  
117 companies some confidence that their methods are sound in  
118 handling electronic data, an inherently interstate activity.  
119 Moreover, it would put all companies on notice that if you  
120 fail to keep up with other companies, if you aren't learning  
121 from other breaches, you will be subject to federal  
122 enforcement.

123       Indeed, too many resources are spent trying to  
124 understand the legal obligations involved with data security  
125 and breach notification. Certainty would allow those  
126 resources to be spent on actual security measures and  
127 notifications and their affected consumers.

128       As we discuss the necessary elements of a data breach  
129 bill, there are a few considerations that I want to mention.  
130 First, there is a limited window for us to act. Criminal  
131 data breaches have grabbed the headlines for about a decade,  
132 but a consensus solution has thus far eluded federal

**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 legislators. This Committee is calling for action, the  
134 President asked for legislation with national breach  
135 notification, and the Senate has legislation in front of it  
136 with a national standard.

137 But most importantly, it is our consumers who are  
138 calling for legislation, thus giving us the time to act.

139 Second, this legislation is limited to this Committee's  
140 jurisdiction. The surest way to deny consumers the benefits  
141 of federal data security legislation is to go into areas  
142 beyond our jurisdiction. Specifically, the health care and  
143 the financial sectors have their own regimes. If we aim to  
144 rewrite rules for those sectors, then it will be years,  
145 perhaps decades, before a bill is signed into law. That is  
146 not to say that we will ignore those issues. But they may  
147 need to be taken up separately.

148 Third, our aspiration at this point is that legislation  
149 comes forward with bipartisan support, and do sincerely  
150 believe that that is an achievable goal.

151 With this hearing, I aim to understand the policy points  
152 where stakeholder compromise is possible. We are seeking to  
153 find agreement not only between the two sides of the dais 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.**

154 also between stakeholders with divergent interests. The  
155 sooner we understand the most important principles, the  
156 smoother negotiations will go over the next several months.

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

158 \*\*\*\*\* 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.**

|

159           Mr. {Burgess.} With that, I do want to thank our  
160 witnesses for the testimonies that they have provided us and  
161 representing their interests candidly in the spirit of  
162 compromise. And I would like to recognize the Vice-Chair of  
163 the Subcommittee, Mr. Leonard Lance, of New Jersey.

164           Mr. {Lance.} Thank you, Mr. Chairman, and it is an  
165 honor to serve under your leadership as the new chair of the  
166 subcommittee, and I am sure you will do a superb job.

167           Well, the debate over data breach legislation has  
168 continued for several years. The issue has been brought to  
169 the forefront by unfortunate, high-profile breaches recently,  
170 and of course, the most recent is the Sony Pictures hack at  
171 the end of last year.

172           The question of how to proceed on data breach reform has  
173 wide implications for both businesses and consumers alike.  
174 Today businesses that attempt to report a breach must  
175 navigate through a complex labyrinth of 47 State laws which  
176 are not all the same. Each State has answered the following  
177 questions in its own way: What is defined as an event  
178 trigger? What is the appropriate timeframe by which

**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.**

179 companies must notify consumers that their identifiable  
180 information has been breached? Who is responsible for  
181 notifying affected consumers?

182       The lack of certainty of these regulations places an  
183 undue burden on businesses trying to report a breach properly  
184 and an undue burden on consumers. Federal law will  
185 streamline regulations, give certainty to businesses  
186 resulting in greater compliance and also to consumers who  
187 suffer a data breach.

188       However, it is my belief that it will only be effective  
189 if it preempts the patchwork of 47 State laws. The debate  
190 over federal data breach legislation has continued over the  
191 span of several Congresses. It is my hope that we can pass  
192 effective, bipartisan data breach legislation this year.

193       Thank you, Mr. Chairman.

194       [The prepared statement of Mr. Lance follows:]

195 \*\*\*\*\* 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.**

|

196           Mr. {Burgess.} The chair thanks the gentleman. The  
197 chair now recognizes the Subcommittee Ranking Member, Ms.  
198 Schakowsky, for 5 minutes for the purpose of an opening  
199 statement.

200           Ms. {Schakowsky.} Thank you, Mr. Chairman, for holding  
201 today's important hearing on what to include in federal  
202 legislative approach to the challenges of data security and  
203 breach notification.

204           I look forward to our work together in the 114th  
205 Congress, and this is a great issue to open up with.

206           The data security is one of the most important issues  
207 that this subcommittee will consider this year. In the State  
208 of the Union last week, the President urged us to pass  
209 legislation that will better protect against cyber attacks  
210 and identity theft. I look forward to working with the White  
211 House and my colleagues on both sides of the aisle to meet  
212 that goal.

213           Since 2005, over 900 million records with personally  
214 identifiable information have been compromised. The recent  
215 uptick in high-profile data breaches including those 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.**

216 Target, Home Depot, Neiman Marcus, and Michael's prove two  
217 important points: One, just about every retailer and many  
218 non-retailers that we engage with are collecting and storing  
219 our personal information, credit card numbers, contact  
220 information, and much more. And two, hackers are growing in  
221 number and becoming more sophisticated in their attempts to  
222 access that personal information, and they are having more  
223 success. From programming home security systems and  
224 thermostats from hundreds of miles away, to remembering  
225 shopping preferences and account information, to connecting  
226 with friends over the internet, Americans benefit in many  
227 ways from an increasingly data-driven world. But that  
228 doesn't mean we should sacrifice our right to have our  
229 personal information appropriately protected or our right to  
230 know if and when that data has been compromised.

231 There are a variety of State laws regarding data  
232 security standards and breach notification requirements.  
233 However, there is no comprehensive federal standard for  
234 appropriate protection of personally identifiable  
235 information, nor are there federal requirements in place to  
236 report data breaches to those whose personal information 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.**

237 been exposed. And I firmly believe that legislation to  
238 address that data breach threat must include those two  
239 safeguards.

240 It is important to say that no legislation to require  
241 data security standards and breach notification will  
242 completely eliminate the threat of data breach. That being  
243 said, entities that collect and store personal information  
244 must take reasonable steps to protect data, and consumers  
245 must be informed promptly in the event of a breach.

246 And while I clearly believe that the Federal Government  
247 should have a role in data breach--that is what we have been  
248 working toward--I also believe that there have been many  
249 important protections that are at the State level that we  
250 don't want to eliminate when we do federal legislation,  
251 perhaps even eliminating rights and protections that would  
252 not be guaranteed under federal statute. We have to be sure  
253 that we don't weaken protections that consumers expect and  
254 deserve. If we include federal preemption of some of those  
255 things or if we don't include those good things in federal  
256 legislation, then I think that would be a serious mistake at  
257 this point.

**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.**

258 I also believe that if we include federal preemption, we  
259 must ensure that State Attorneys General are able to enforce  
260 the law, something my Attorney General has made very, very  
261 clear.

262 So I think we can achieve all these goals working  
263 together, get a good, strong federal bill that makes  
264 consumers feel confident that we have taken the appropriate  
265 steps.

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

267 \*\*\*\*\* 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.**

|

268 Ms. {Schakowsky.} And let me with my remaining time  
269 yield to Peter Welch for his comments.

270 Mr. {Welch.} Thank you very much. Mr. Chairman and  
271 Ranking Member, you both nailed it with your description of  
272 what we are doing. It is pretty astonishing that with the  
273 use of computers, two things still have not been done at the  
274 federal level: one, to provide data breach security, and  
275 number two, to provide notice to consumers. Consumers  
276 receive notice when they have been harmed, but they don't  
277 need notice just to scare them. And we have bipartisan  
278 momentum here, thanks to Chairman Upton and my colleague  
279 Marsha Blackburn, who I have been working with, and  
280 Congressman Rush has been working on this for a long time.  
281 So we have got a foundation here.

282 The practical challenges, those are the ones we have to  
283 resolve. What do we do about a national standard? What do  
284 we do about having enforcement at the AG level, something I  
285 agree with Ms. Schakowsky on. What is the notice standard?  
286 When should consumers be notified? How do you give some time  
287 for a company that has been breached to do law enforcement,



**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.**

288 investigation, and inquiry into what the scope of the breach  
289 was? These are more or less practical issues. And I think  
290 the chairman has set a good tone here where we have a common  
291 objective, and we don't have ideological differences. We  
292 have practical differences. And the hope I think of all of  
293 us with the foundation that has been laid by my predecessors  
294 is to find some common-sense, legitimate balancing of the  
295 interests so that at the end of the day we do protect  
296 consumers with data breach security, we give some reasonable  
297 certainty to our companies, and we have a standard that is  
298 robust and strong. I yield back.

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

300 \*\*\*\*\* 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.**

|

301           Mr. {Burgess.} I thank the gentleman. The gentleman  
302 yields back. The chair now recognizes the Chairman of the  
303 Full Committee, Mr. Upton, for 5 minutes for an opening  
304 statement.

305           The {Chairman.} Thank you, Mr. Chairman, and it has  
306 been noted this committee does have a strong tradition of  
307 bipartisan cooperation and problem solving. In this spirit,  
308 today we continue our focus on the key elements to pass a  
309 federal data breach law, a priority that the President  
310 identified in his State of the Union address just last week.  
311 I look forward to working with the White House, Dr. Burgess,  
312 and members of this committee on both sides of the aisle to  
313 accomplish that goal.

314           Criminal cyber hacking presents a serious risk of  
315 economic harm to consumers and businesses alike. From small  
316 mom-and-pop shops in my district in Southwest Michigan to  
317 global Fortune 100 companies, the unfortunate reality is that  
318 companies of all sizes are at risk of having information  
319 hacked.

320           This committee will be examining a series of 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.**

321 relating to cybersecurity in this Congress. Where the  
322 conversation begins today is with a data breach bill, and I  
323 want to encourage all members and the public to focus on  
324 getting that issue right before we try to tackle some of the  
325 other concerns. There are significant privacy issues in an  
326 online economy, and some of those will have to be addressed  
327 separately.

328 Let us also be clear that this isn't a financial  
329 services bill. We cannot let data breach legislation be sunk  
330 by extraneous issues.

331 Today's hearing will examine two discrete issues related  
332 to the complex effects of cybercrime, commercial data  
333 security and breach notification to consumers. There is a  
334 real opportunity this Congress to set a single, national  
335 standard for data security and breach notification. I  
336 personally believe that a single, federal standard is the key  
337 to passing a solution. The trade-off is that it has to be a  
338 strong, consumer-friendly law, one that has real protections  
339 and real enforcement. Both the FTC and State AGs have shown  
340 that this is an area that they would police very effectively.  
341 Our role is to strike the right balance on when 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.**

342 is required, how timely it needs to be, and what information  
343 leads to identity theft.

344           Setting a national standard benefits consumers by  
345 ensuring that every business must look at their activities  
346 and make certain that they are taking reasonable security  
347 measures. A national standard allows businesses to focus on  
348 securing information and systems instead of trying to figure  
349 out how to comply with a host of different State laws with  
350 their team of lawyers. Consumers benefit from consistency as  
351 well.

352           We are particularly concerned with the impact that these  
353 criminal acts have on consumer confidence, economic growth,  
354 and job creation. So let us get to work. A data breach bill  
355 is the first step in securing that future.

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

357 \*\*\*\*\* 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.**

|

358           The {Chairman.} I yield the balance of my time to the  
359 Vice-Chair of the Full Committee, Marsha Blackburn.

360           Mrs. {Blackburn.} Thank you, Mr. Chairman, and I want  
361 to thank the chairman of the subcommittee for calling the  
362 hearing, and I want to welcome all of our witnesses today.  
363 We are indeed looking forward to hearing what you have to  
364 say.

365           As has been referenced by Mr. Welch, we have spent a  
366 couple of years working on the issues of privacy and data  
367 security. We have done this in a working group or a task  
368 force and drilling down, making certain that we have a good  
369 understanding of defining the problem and then looking at the  
370 opportunities for addressing that. So we come to you from  
371 that basis of work. And Ms. Schakowsky, Mr. Olson, both  
372 served on this task force with us.

373           Last October Director Comey from the FBI said there are  
374 two kinds of big companies in the United States: those that  
375 know they have been hacked by the Chinese and those that  
376 don't know they have been hacked by the Chinese. That is  
377 pretty apropos, and we know that it applies to all sizes 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.**

378 companies, as Chairman Upton just said.

379           Because of that, we understand that there are a few  
380 things that we need to look at: preemption and making  
381 certain that we have the standard, that this is easily  
382 communicated, that our constituents and the citizens  
383 understand what is the toolbox that they have for protecting,  
384 as I define it, the virtual you, whether that virtual you is  
385 they themselves individually, they themselves the small  
386 business person, or the corporate entity that is looking to  
387 protect its product and its name.

388           Now, I come from Nashville. We have a lot of  
389 entertainment, healthcare, and financial services that are  
390 watching this issue closely. They want to make certain that  
391 we get this right the first time.

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

393 \*\*\*\*\* 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.**

|

394 Mrs. {Blackburn.} With that, I yield back the balance  
395 of my time.

396 Mr. {Burgess.} The gentlelady yields back. The chair  
397 now recognizes the Ranking Member of the Full Committee, 5  
398 minutes for an opening statement, Mr. Pallone from New  
399 Jersey.

400 Mr. {Pallone.} Thank you, Mr. Chairman. I first wanted  
401 to congratulate Dr. Burgess on his appointment as the  
402 chairman. I will say, though, that having spent last evening  
403 with you on rules, I am not going to congratulate you on  
404 continuing on rules because I don't know what possible reason  
405 you could have for continuing to stay there. But everyone  
406 makes their own decisions around here.

407 I do look forward to working with you on many issues,  
408 starting with the issue of today's hearing, data security and  
409 breach notification. I also wanted to thank Ms. Schakowsky  
410 for her continued service as the Democratic Ranking Member.

411 The title of this hearing, What are the Elements of  
412 Sound Data Breach Legislation?, assumes that legislation is  
413 needed, and I agree that it is time to legislate but only 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.**

414 the result is a strong bill that puts consumers in a better  
415 place than they are today. Right now millions of consumers  
416 are being hit with endless waves of breaches. Criminal  
417 hackers will always target our communities, and while we  
418 cannot expect to eliminate data breaches, we can work harder  
419 to reduce the number of breaches and better protect  
420 consumers' information. Just as we expect a bank to lock its  
421 vaults of money, we should expect that companies lock and  
422 secure personal consumer information. Unfortunately, that is  
423 not happening. According to the Online Trust Alliance, over  
424 90 percent of data breaches in the first half of 2014 could  
425 have been prevented had businesses implemented security best  
426 practices. Firms must do a better job of protecting  
427 information they demand of consumers, and preventing breaches  
428 is not just best for the consumer, in the long run it is  
429 cheaper for companies as well.

430 And I believe that we should also expect companies to  
431 notify consumers in the event of a breach. During this  
432 hearing we will hear the often-repeated statistic that 47  
433 States plus Washington, D.C., Guam, Puerto Rico, and the  
434 Virgin Islands already have data breach notification laws 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.**

435 the books. While no one on either side of the aisle wants to  
436 unnecessarily burden businesses with duplicative or  
437 overlapping requirements, these State laws provide baseline  
438 breach notification to most Americans. In addition,  
439 businesses that operate nationally often follow the strictest  
440 state laws, giving our constituents strong data security and  
441 breach notification protections coverage regardless of what  
442 is written in any individual State law. And therefore, I  
443 can't support any proposal that supersedes strong State  
444 protections and replaces them with one weak federal standard.

445 So Mr. Chairman, this subcommittee has had a tradition  
446 of being bipartisan, particularly on the issue of data  
447 security, and the 111th Congress' committee passed a  
448 compromise bill on the House Floor as H.R. 2221, and that  
449 bill was shepherded by then-Subcommittee Chairman Bobby Rush  
450 and was based on a bill crafted by former Subcommittee  
451 Chairman Cliff Stearns, and Chairman Upton, Vice-Chairwoman  
452 Blackburn, and Chairman Barton were original cosponsors of  
453 these various bills.

454 So I just want to say I look forward to working with the  
455 subcommittee on a bipartisan basis to craft similar

**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.**

456 legislation and legislation that requires companies to have  
457 reasonable security measures in place and to provide  
458 notification to consumers once a breach has occurred.

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

460 \*\*\*\*\* 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.**

|

461 Mr. {Pallone.} I yield back, Mr. Chairman.

462 Mr. {Burgess.} The gentleman yields back his time. The  
463 chair would remind all members on the subcommittee that they  
464 are able to insert their written statements for the record.

465 And I do want to welcome our witnesses for being here  
466 this morning. I thank all of you for agreeing to testify  
467 before the committee. Our witness panel for today's hearing  
468 will include Ms. Elizabeth Hyman who is the Executive Vice  
469 President of Public Advocacy for TechAmerica, and she will be  
470 testifying on behalf of the Computing Technology Industry  
471 Association. We also have Ms. Jennifer Glasgow, the Global  
472 Privacy Officer for Acxiom Corporation; Mr. Brian Dodge, who  
473 is the Executive Vice President of Communications and  
474 Strategic Initiatives on behalf of the Retail Industry  
475 Leaders Association; and Mr. Woodrow Hartzog, an Associate  
476 Professor of Law at Samford University's Cumberland School of  
477 Law in Birmingham, Alabama.

478 Our first witness is Ms. Elizabeth Hyman, and you are  
479 recognized for 5 minutes.

**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.**

|

480 ^STATEMENTS OF ELIZABETH HYMAN, EXECUTIVE VICE PRESIDENT,  
481 PUBLIC POLICY, TECH AMERICA; BRIAN DODGE, EXECUTIVE VICE  
482 PRESIDENT, COMMUNICATIONS AND STRATEGIC INITIATIVES, RETAIL  
483 INDUSTRY LEADERS ASSOCIATION; JENNIFER BARRETT-GLASGOW, CHIEF  
484 PRIVACY OFFICER, ACXIOM CORPORATION; AND WOODROW HARTZOG,  
485 ASSOCIATE PROFESSOR, SAMFORD UNIVERSITY, CUMBERLAND SCHOOL OF  
486 LAW.

|

487 ^STATEMENT OF ELIZABETH HYMAN

488 } Ms. {Hyman.} Thank you, Mr. Chairman.

489 Mr. {Burgess.} Be certain that your microphone is--

490 Ms. {Hyman.} Sorry about that. There we go. Fair  
491 enough. Good morning, and thank you very much for having us,  
492 Chairman Burgess, Ranking Member Schakowsky, and  
493 distinguished members of the Subcommittee on Commerce,  
494 Manufacturing, and Trade. We appreciate your convening this  
495 hearing and for giving us the opportunity to provide our  
496 insights on the important issue of consumer data breach  
497 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.**

498           My name as you mentioned is Elizabeth Hyman. I am the  
499 Executive Vice President of Public Advocacy for TechAmerica,  
500 the public policy department of The Computing Technology  
501 Industry Association, CompTIA. CompTIA is headquartered in  
502 Downers Grove, Illinois, and we represent over 2,200  
503 technology companies, a large number of which are small- and  
504 medium-sized firms.

505           Technology companies take their obligations to protect  
506 consumers' information very seriously. Data is the life-  
507 blood of the internet economy, and protecting consumers'  
508 information is not only a responsibility of the industry but  
509 also a crucial business practice. Failure to do so will lead  
510 to a loss in customer faith and damage to a business'  
511 reputation.

512           Unfortunately, as has been pointed out, criminals remain  
513 intent on stealing information. Data breaches are sadly all  
514 too common in 2015, and thus we need strong rules in place to  
515 inform consumers when a harmful breach occurs and to provide  
516 the necessary information to enable consumers to take the  
517 necessary steps to protect themselves.

518           As you are all well aware and has been stated, there

**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.**

519 currently is no federal standard for data breach  
520 notification. Instead, 47 different States, the District of  
521 Columbia, Puerto Rico, Guam, and the Virgin Islands, all have  
522 their own separate data breach notification laws and  
523 requirements.

524 Furthermore, States are regularly changing and updating  
525 their data breach notification laws. This year we have  
526 already seen 17 bills introduced in seven States in just the  
527 first 2 weeks of State legislative sessions. With the  
528 increasingly mobile and decentralized nature of our economy,  
529 most companies are under the umbrella of multiple State laws  
530 at all times. This patchwork of state laws creates  
531 significant compliance costs with no additional protection  
532 for consumers since no two State data breach laws are exactly  
533 the same. In fact, many are in conflict with one another. A  
534 federal data breach notification standard is thus necessary  
535 to protect consumers and ensure that companies can respond  
536 quickly and effectively after a breach.

537 Responding to a data breach for a company of any size is  
538 difficult, especially given the need to assess whether the  
539 breach could trigger notification provisions in any one of 47

**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.**

540 States, whether they have any consumers that live in any of  
541 those States, who to notify, how to notify, what information  
542 to include, and what the timelines are for notification.

543 Small- and medium-sized businesses face particularly  
544 difficult compliance challenges. To address their  
545 obligations to resolve the breach, gather information, and  
546 notify the necessary parties, these companies often rely on  
547 cyber-insurance, payment processors, or outside counsel to  
548 help implement a response plan. None of these options is  
549 cheap.

550 Thus, the key to any federal data breach notification  
551 law will be finding a single standard that maintains strong  
552 requirements but allows companies to focus on the important  
553 work of protecting their customers in the wake of a breach.

554 In crafting a federal data breach standard, we would  
555 suggest a few key provisions that are further outlined in my  
556 statement for the record. For example, any federal data  
557 breach notification law needs to be the standard for all  
558 companies to comply with. It cannot simply just become the  
559 48th standard that State can add to. In order to avoid the  
560 risks associated with over-notification, a federal standard

**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.**

561 should ensure that consumers only receive notification about  
562 a breach when their information has actually been accessed  
563 and only when that information is likely to be used in a  
564 harmful manner.

565 Adequate time should be provided for companies to  
566 conduct a risk assessment in order to best assess the scope  
567 and depth of the breach. A circumscribed set of sensitive,  
568 personally identifiable information must be the basis for  
569 determining whether any notification should occur. We should  
570 try to avoid mandating specific technologies while also  
571 exempting companies from notification requirements where data  
572 is rendered unusable. Companies should not be punished for  
573 the criminal acts of others, and private rights of action  
574 regarding data breach notification should be explicitly  
575 banned.

576 In closing, I would like to thank the subcommittee for  
577 working on the issue of data breach notification.  
578 Unfortunately, our patchwork of state laws, while well-  
579 intentioned, has created a burdensome and complex compliance  
580 regime. A strong, single standard that applies throughout  
581 the country will ensure our consumers are safer and ensure



**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.**

582 our companies are well-informed about how to respond to the  
583 growing threat of data breaches.

584 Security and economic growth are not mutually exclusive,  
585 and I would respectfully request that the solutions you draft  
586 through this subcommittee address both through a national  
587 data breach notification standard. Thank you.

588 [The prepared statement of Ms. Hyman follows:]

589 \*\*\*\*\* INSERT 1 \*\*\*\*\*

**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.**

|

590           Mr. {Burgess.} The gentlelady yields back. The chair  
591 would now recognize Mr. Brian Dodge, the Executive Vice  
592 President of the Retail Industry Leaders Association, 5  
593 minutes for your testimony, sir. Thank 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.**

|

594 ^STATEMENT OF BRIAN DODGE

595 } Mr. {Dodge.} Chairman Burgess, Ranking Member  
596 Schakowsky, and Members of the committee, my name is Brian  
597 Dodge, and I am an Executive Vice President with the Retail  
598 Industry Leaders Association. Thank you for the opportunity  
599 to testify today about data breach legislation and the steps  
600 that the retail industry is taking to address this important  
601 issue and to protect consumers.

602 RILA is the trade association of the world's largest and  
603 most innovative companies. Retailers embrace innovative  
604 technology to provide American consumers with unparalleled  
605 services and products. While technology presents great  
606 opportunity, nation states, criminal organizations, and other  
607 bad actors also are using it to attack businesses,  
608 institutions, and governments. As we have seen, no  
609 organization is immune from attacks. Retailers understand  
610 that defense against cyber attacks must be an ongoing effort.

611 RILA is committed to working with Congress to give  
612 government and retailers the tools necessary to thwart this

**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.**

613 unprecedented attack on the U.S. economy and bring the fight  
614 to cybercriminals around the world.

615         As leaders in the retail community, we are taking new  
616 and significant steps to enhance cybersecurity throughout the  
617 industry. To that end, last year RILA formed the Retail  
618 Cyber Intelligence Sharing Center in partnership with  
619 America's most recognized retailers. The Center has opened a  
620 steady flow of information between retailers, law enforcement  
621 and other relevant stakeholders.

622         In addition to the topics this hearing will cover today,  
623 one area of security that needs immediate attention is  
624 payment card technology. The woefully outdated magnetic  
625 stripe technology used on cards today is the chief  
626 vulnerability in the payments ecosystem. Retailers continue  
627 to press banks and card networks to provide U.S. consumers  
628 with the same chip and PIN technology that has proven to  
629 dramatically reduce fraud when it has been deployed elsewhere  
630 around the world.

631         Before I discuss what RILA believes the components of  
632 sound data breach legislation are, I will briefly highlight  
633 the significant data breach and data notification laws with

**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.**

634 which retailers currently comply. As has been said, 47  
635 States, the District of Columbia, Guam, Puerto Rico, and the  
636 U.S. Virgin Islands have adopted data breach notification  
637 laws. In addition to the 47-plus existing State data breach  
638 notice laws, retailers are subject to robust data security  
639 regulatory regimes as well. The Federal Trade Commission has  
640 settled at least 50 cases against businesses that it charged  
641 with failing to maintain reasonable data security practices.  
642 These actions have created a common law of consent decrees  
643 that signal the data security standards expected of  
644 businesses. Additionally, inadequate data security measures  
645 for personal information can lead to violations of expressed  
646 State data security laws. Also, many States has so-called  
647 little FTC acts that can be used to enforce against what  
648 Attorneys General deem to be unreasonable data security  
649 practices.

650 Finally, retailers voluntarily and by contract follow a  
651 variety of security standards including those maintained by  
652 the payment card industry, NIST, and the International  
653 Organization of Standardization.

654 While retailers diligently comply with this range 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.**

655 data security notice and data requirements, a carefully  
656 crafted federal data breach law can clear up regulatory  
657 confusion and better protect and notify consumers.

658 RILA supports a federal data breach that is practical,  
659 proportional, and sets a single national standard. RILA  
660 urges the committee to consider data breach legislation that  
661 creates a single national notification standard that allows  
662 business to focus on quickly providing affected individuals  
663 with actionable information; that provides flexibility in the  
664 method and timing of notification; that ensures that notice  
665 is required only when there is a reasonable belief that the  
666 breach has or will result in identity theft, economic loss,  
667 or harm; that ensures that the responsibility to notify is  
668 that of the entity breached but provides the flexibility for  
669 entities to contractually determine the notifying party; that  
670 establishes a precise and targeted definition for personal  
671 information; that recognizes that retailers already have  
672 robust data security obligations and that security must be  
673 able to adapt over time.

674 The final goal of data breach legislation should be to  
675 ensure fair, consistent, and equitable enforcement of 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.**

676 breach law. Enforcement of the law should be consistently  
677 applied by the FTC based on cases of actual harm. Similarly,  
678 if civil penalty authority is provided, it should be capped  
679 based on the actual harm to consumers. Also, any legislation  
680 should deny a private right of action as it would undermine  
681 consistent enforcement.

682           We look forward to working with the committee on  
683 specific language to address each of these above goals. I  
684 thank the Committee for considering the need for preemptive  
685 data breach legislation and look forward to answering your  
686 questions.

687           [The prepared statement of Mr. Dodge follows:]

688 \*\*\*\*\* INSERT 2 \*\*\*\*\*

**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.**

|

689           Mr. {Burgess.} The gentleman yields back. The chair  
690 would now like to recognize Jennifer Barrett-Glasgow, the  
691 Global Privacy Officer for the Acxiom Corporation. Thank you  
692 for your testimony today, 5 minutes.



**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.**

|

693 ^STATEMENT OF JENNIFER BARRETT-GLASGOW

694 } Ms. {Barrett-Glasgow.} Chairman Burgess, Ranking Member  
695 Schakowsky, members of the committee, thank you for holding  
696 this hearing today. I am Jennifer Barrett-Glasgow, Global  
697 Privacy Officer for Acxiom, headquartered in Little Rock,  
698 Arkansas. Acxiom has two lines of business. We offer  
699 primarily to large businesses, not-for-profit organizations,  
700 political parties, and candidates and government agencies.  
701 First, we offer computer processing services for our clients'  
702 information which includes ensuring that information is  
703 accurate, analyzing the information to help our clients  
704 understand their customers better so they can improve their  
705 offerings, and our digital reach services which enable our  
706 clients to market to audiences across all digital channels.  
707 These services represent over 80 percent of our total  
708 business in the United States.

709 Second, we provide a line of information products to  
710 clients in three categories: fraud management, telephone  
711 directories, and marketing. And these products support all

**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.**

712 channels of communication, offline, online, mobile, and  
713 addressable television.

714 Acxiom supports enacting a data security and breach  
715 notification bill, and I would like to mention some of the  
716 provisions that we think should and should not be included.  
717 Regarding data breach notification provisions, first, the  
718 bill needs to include strong preemption for State laws. As  
719 stated earlier, 47 States and 4 territories have breach laws,  
720 and every year a number of these change. Businesses and  
721 consumers will benefit from having one recognizable standard.

722 Second, there should be a harm-based trigger for  
723 notification. Consumers shouldn't get meaningless notices  
724 when there is no risk of harm. Businesses will have to  
725 evaluate whether there is a reasonable risk if there are  
726 penalties for failing to notify, and we will do that  
727 responsibly without Congress needing to spell out how it  
728 should be done.

729 Third, legislation should also provide a reasonable  
730 timeframe for notification. Consumers do need to be notified  
731 promptly, but it is critical to understand the extent and  
732 means of the breach and to give law enforcement time 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.**

733 identify and hopefully even apprehend the bad guys. Fixed  
734 statutory deadlines do not accomplish these objectives.

735 Fourth, penalty provisions should be reasonable, and we  
736 do not believe there should be a private right of action.  
737 Companies who take reasonable precautions but who still get  
738 breached are victims, too. Regarding data security language,  
739 just as with breach notification, having a single data  
740 security standard is more efficient for companies than  
741 multiple State standards. This is more important for some  
742 businesses and other entities than it is for Acxiom. We  
743 process data for other companies, and our security is  
744 assessed by clients upwards of 80 times a year, plus we  
745 conduct our own audit internally. So we already meet  
746 multiple client standards in addition to those set by law.

747 Next, because the bad guys' capabilities keep changing,  
748 legal and regulatory data security standards need to be  
749 extremely flexible to allow adaptive compliance to keep ahead  
750 of the threats.

751 And last, Acxiom believes that businesses have a  
752 responsibility to educate their employees about security  
753 risks and that government has a role to play in educating 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.**

754 general public on these topics.

755       Where once the purpose of passing a data security law  
756 might have been to ensure companies were thinking enough  
757 about security, today we believe Congress should think about  
758 security breach legislation more like it has thought about  
759 cybersecurity legislation. How can the industry and  
760 government and law enforcement work together to keep ahead of  
761 these threats.

762       Finally, a comment on what should not be included in  
763 this legislation. Congress should keep this bill focused on  
764 data security and breach notification. There is bipartisan  
765 support for enacting a good bill into law on these issues.  
766 In the past, other issues have crept into data breach bills,  
767 and this has hurt the chances of enactment. For example,  
768 some previous bills have included provisions for data  
769 brokers, and while Acxiom would be considered a data broker  
770 under any definition, it already offers the kinds of  
771 provisions seen in past bills through our web portal,  
772 AboutTheData.com. The problem has been the definition of  
773 data brokers. It was quite broad and included many companies  
774 that don't consider themselves to be one. This has stymied

**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.**

775 enactment of these bills. We urge you to keep the bill clean  
776 so we can finally put a good consensus federal data security  
777 and breach notification law into place.

778 Thank you for the opportunity to testify today, and I  
779 look forward to your questions.

780 [The prepared statement of Ms. Barrett-Glasgow follows:]

781 \*\*\*\*\* INSERT 3 \*\*\*\*\*

**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.**

|

782           Mr. {Burgess.} Thank you. The witness yields back.

783 The chair now recognizes Mr. Hartzog, 5 minutes for your

784 testimony. Thank you, sir, for being here.

**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.**

|

785 ^STATEMENT OF WOODROW HARTZOG

786 } Mr. {Hartzog.} Thank you. Chairman Burgess, Ranking  
787 Member Schakowsky, and Members of the Committee, thank you  
788 very much for inviting me to appear before you and provide  
789 testimony. My name is Woodrow Hartzog, and I am an associate  
790 professor of law at Samford University's Cumberland School of  
791 Law and an affiliate scholar at the Center for Internet and  
792 Society at Stanford Law School. I have spent the last 3  
793 years researching the law and policy of data protection, data  
794 security, and responses to data breaches. My comments today  
795 will address what I have learned from this research.

796 In order to be sound, data breach legislation must  
797 further three fundamental goals: transparency, data  
798 protection, and remedies for affected individuals. The  
799 patchwork of existing State and federal sector-specific laws  
800 further these goals, but aggressively preemptive federal  
801 legislation risks counteracting these goals and weakening our  
802 critical data protection infrastructure. Hard-won consumer  
803 protections could be lost. In short, any data breach

**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.**

804 legislation that fails to advance these three goals will be  
805 counterproductive.

806 I would like to make two main points regarding the  
807 elements of sound data breach legislation. First, sound data  
808 breach legislation should be minimally preemptive of existing  
809 State- and sector-specific data breach laws. Data breach  
810 laws are relatively new. It is not yet clear what the most  
811 effective approach to data protection and data response is or  
812 should be. We need multiple regulatory bodies to ensure the  
813 adequate resources and experimentation necessary to respond  
814 to constantly evolving threats and new vulnerabilities.  
815 Additionally, preemption threatens to water down important  
816 existing robust data breach protections. There is a real  
817 risk that preemptive federal legislation would do more harm  
818 than good. For example, federal data breach legislation  
819 would reduce the level of protection many or most Americans  
820 currently have if it narrowed existing definitions of  
821 personal information, if it mandated a showing of harm before  
822 companies were required to send notification, or if it failed  
823 to require a notice to a centralized organization, like the  
824 office of the State Attorney General.



**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.**

825           Data breach legislation would also be counter-productive  
826 if it created gaps in protection. Federal data breach  
827 legislation that preempts all state data breach laws could  
828 fail to cover data breaches that only affect the residents of  
829 one State. Additionally, preemptive legislation that only  
830 covered digitized records would fail to cover breaches  
831 involving paper records which remain a significant target for  
832 data thieves.

833           The second point I would like to make is that sound data  
834 breach legislation must also incorporate requirements for  
835 data security. While data breach notification is important,  
836 we must be sure not to ask too much of it. Under a pure data  
837 breach notification scheme, providing reasonable data  
838 security would be voluntary. The law should require not just  
839 encourage that companies reasonably secure their personal  
840 data. If people cannot trust that the entities that collect  
841 and store our personal information, the commerce, innovation,  
842 public health, our personal relationships, and our culture  
843 will all suffer. Ensuring that companies must provide  
844 reasonable data security will ensure that fewer breach  
845 notifications need to be sent at all.

**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.**

846           One important way to fortify data security would be to  
847 give the Federal Trade Commission rule-making authority.  
848 Specific authority for data security would help the FTC  
849 further clarify data security standards, require data  
850 security from non-profit entities such as educational  
851 institutions, and issue civil penalties.

852           Federal legislation should also preserve the regulation  
853 of data security by States and sector-specific agencies. The  
854 numerous federal agencies that require data security are not  
855 redundant. Rather, they can and do coexist with unique  
856 expertise and regulatory authority. Even agencies with  
857 overlapping jurisdiction contribute valuable resources and  
858 have relatively harmonized approaches to data security.

859           Finally, data breach legislation must preserve the  
860 ability of States to regulate data security. Data security  
861 is both a national and a local issue sometimes affecting  
862 small but significant groups of State residents. Even in the  
863 case of large national breaches, residents of some States are  
864 hit harder than others. States are nimble and capable of  
865 continued experimentation regarding the best approach to  
866 regulating data security. They are also closer to those

**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.**

867 whose data was compromised and provide additional resources  
868 to alleviate the strain and cost to enforcement on federal  
869 agencies.

870           The modern threat to personal data is still relatively  
871 new. The concept of data breach legislation is newer still.  
872 It is too early to start rolling back protections and  
873 consolidating agencies to cut costs. Instead, sound data  
874 breach legislation should reinforce the current trajectory of  
875 data breach law which involves multiple approaches and  
876 constantly evolving robust consumer protection. Thank you  
877 very much, and I look forward to your questions.

878           [The prepared statement of Mr. Hartzog follows:]

879 \*\*\*\*\* INSERT 4 \*\*\*\*\*

**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.**

|

880           Mr. {Burgess.} The gentleman yields back, and I thank  
881 all the witnesses for their testimony and participating in  
882 today's hearing. We will now move into the question-and-  
883 answer portion of the hearing, and for that purpose, I will  
884 recognize myself for 5 minutes. And I do again thank you all  
885 for being here.

886           Let me just ask a general question to the entire panel,  
887 and we will start with Ms. Hyman and work our way down to Ms.  
888 Hartzog. Reading through the testimony and listening to you  
889 this morning, it is clear that most of the panelists agree  
890 on--I guess I could say three out of four panelists agree on  
891 preemption, that it is necessary for a successful piece of  
892 legislation on data security and breach notification. The  
893 question is why is it important to have a single standard  
894 rather than allowing new requirements to be developed in  
895 State courts on top of a federal law? Ms. Hyman, let us  
896 start with you.

897           Ms. {Hyman.} Thank you, Chairman Burgess. It is  
898 important because right now we have all these different laws,  
899 many of which are in conflict with one another. Many of our

**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.**

900 member companies are small- and medium-sized IT firms, and  
901 they are trying to do business across State lines. They  
902 don't necessarily have the in-house resources to cover all  
903 the different State requirements. So having a more  
904 simplified federal standard, strong but a federal standard,  
905 would allow these companies to do business across State lines  
906 with confidence that they are serving their consumers.

907       The only other thing I would point out is, and I  
908 mentioned this in my opening remarks, this is a very  
909 unsettled area. As I mentioned just in the last couple of  
910 weeks, we have seen a number of bills introduced in State  
911 legislatures, and again, if there is some way that we can  
912 come up with a strong, appropriate federal standard, I think  
913 it would alleviate a fair amount of ambiguity for both the  
914 consumer and for the business.

915       Mr. {Burgess.} Thank you. Mr. Dodge?

916       Mr. {Dodge.} So I would say the States deserve a lot of  
917 credit for acting in the place where the Federal Government  
918 hasn't yet. But if Congress intends to or chooses to pass a  
919 federal standard, we believe it should be preemptive because  
920 first, it will allow consumers to have a clear set 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.**

921 expectations regardless of where they live about what kind of  
922 notification they will get, at what time post-breach. We  
923 think that is important. Consumers need to know what to  
924 expect in the wake of a breach. And also for a breach of  
925 institution or business, they want to put all of their energy  
926 towards making sure they are quickly communicating actionable  
927 information to the consumers. And a national standard would  
928 allow them to do that instead of the complexity of complying  
929 with 47-plus different laws.

930 Mr. {Burgess.} Ms. Glasgow?

931 Ms. {Barrett-Glasgow.} Breach notification laws that  
932 are in place today in the States vary widely as has been  
933 said, and in some instances, we don't even have a security  
934 requirement in certain State laws. So enacting a federal law  
935 that includes both a security requirement and a breach  
936 notification requirement will raise the level across the  
937 country. And I think if you study those laws to any great  
938 degree, you will find that there are very few exceptions that  
939 would make a state regime more protective from any consumers.

940 Secondly, from a consumer perspective, we don't live  
941 in one State all our lives often. I grew up in Texas 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.**

942 moved to Arkansas. And different States with different  
943 regimes with different requirements for the types of notices  
944 that need to be given create inconsistency for the consumer  
945 if they happen to have received a notice in one State and  
946 then receive a different notice in another State. As I said  
947 in my testimony, I hope that we will look at much more  
948 cooperation between law enforcement and companies to educate  
949 consumers about the risks that are out there so that they can  
950 help in protecting themselves and not rely solely on  
951 companies or government notifying them when there has been a  
952 problem.

953 Mr. {Burgess.} Thank you. Mr. Hartzog?

954 Mr. {Hartzog.} So I think that preemption on a very  
955 limited scale could actually be useful. I think the  
956 important thing to remember is that preemption is not an all-  
957 or-nothing game, right? So we can preempt minimally or we  
958 can have aggressive preemption. So one of the reasons I  
959 recommend minimal preemption is so we can move closer towards  
960 having a national standard but then preserve some of the  
961 hard-won consumer protections and also make sure that federal  
962 legislation doesn't create gaps that things that were

**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.**

963 protected are no longer protected, so for example, solely  
964 interstate, intrastate data breaches. And I think that as  
965 far as the differences between the 47 different pieces of  
966 legislation, they do vary, but I think that maybe sometimes  
967 the differences can be overstated possibly. I mean, I think  
968 that sometimes it is compared so that it is apples to  
969 oranges, which I don't think is true. I think the more  
970 appropriate metaphor might be Fuji to red delicious apples,  
971 and the idea that it is very burdensome to comply with all 47  
972 State laws, I think that is also possibly, potentially an  
973 overstated claim in the sense that (a) businesses comply with  
974 50 different State laws all the time, and (b) a very robust  
975 support network exists to provide companies of all sizes with  
976 the adequate help they need to respond to data breach  
977 requirements.

978 Mr. {Burgess.} I thank the gentleman. The chair now  
979 recognizes Ms. Schakowsky, 5 minutes for the purposes of  
980 questions.

981 Ms. {Schakowsky.} Thank you. Professor, I wanted to  
982 direct my question to you. Authors of some State laws and  
983 some federal legislative proposals have chosen to 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.**

984 notification to consumers to be determined by a standard in  
985 which notification is dependent on the presence of a risk of  
986 harm or actual financial harm to consumers. And I am just  
987 wondering if you are concerned about harms beyond identity  
988 theft, fraud, or other economic loss, and if so, if you could  
989 give us some examples that might narrow too much the  
990 definition of risk.

991         Mr. {Hartzog.} Sure. Thank you very much. I think  
992 that the harm trigger as it has been described, the idea that  
993 you only have to notify if there is some kind of finding of  
994 harm, is a dubious proposition in several different ways,  
995 mainly because the concept of harm within privacy law is  
996 hotly contested, and to limit the idea of harm to something  
997 like financial harm I think is really constraining because  
998 there are lots of different harm that can result from data  
999 breaches. So fraud and identity theft are not the only two.  
1000 When health data gets stolen, you risk things like  
1001 discrimination, adverse employment decisions, emotional  
1002 distress. The Sony hack made it very clear that sometimes  
1003 when information is breached, it is not used to commit  
1004 financial harm. It is posted online for everyone to see.

**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.**

1005           And so that brings me to my next point which is the harm  
1006 trigger is dubious mainly because it is very difficult to  
1007 draw a line of causation between a breach that occurred and  
1008 likely harm that can happen sometime in the future. So it is  
1009 not as though data gets stolen and it is a one-to-one that  
1010 harm occurs as a result of it. Oftentimes data gets flooded  
1011 downstream and aggregated with other pieces of data, and it  
1012 can be extremely difficult to meet the burden of proof that  
1013 harm is actually likely in any one particular instance. And  
1014 when you mandate a harm trigger in notification, then what  
1015 that means is if you don't have enough information to prove  
1016 some kind of likelihood of harm, which is often the case in  
1017 many different kinds of data breaches, then the harm doesn't  
1018 go out. So as a matter of default, the notification isn't  
1019 extended.

1020           And so I think that it is important to remember the many  
1021 different ways in which harm can occur and the many different  
1022 ways in which harm is a relatively dubious concept within  
1023 data breach law, not the least of which is that we haven't  
1024 even talked about the ways in which information can be used  
1025 against people, not just to harm you for identity theft

**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.**

1026 purposes but to trick you into revealing more information.  
1027 This is a common phishing attack, right, which is what they  
1028 call where they use your own personal information into  
1029 tricking you into think this is a communication from a  
1030 trusted source. You click on it, then disclose more personal  
1031 information. And this is more than just a threat to the  
1032 individual who is tricked. One of the most common ways to  
1033 hack into companies is through exploiting human  
1034 vulnerabilities, and one of the ways in which we do that is  
1035 we take information about people and use that to trick them  
1036 into revealing more information.

1037 Ms. {Schakowsky.} Answer a question then. Is there a  
1038 way to identify harm or define harm that would include  
1039 everything you are talking about? Or are you saying that a  
1040 harm trigger itself? In other words, what you are suggesting  
1041 is there needs to be notification of a breach without having  
1042 to establish harm at all or are you saying we need to define  
1043 harm better?

1044 Mr. {Hartzog.} That is correct. So generally speaking,  
1045 I want to caution against over-leveraging the concept of  
1046 harm, and the easiest way to over-leverage the concept 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.**

1047 harm is to create a harm trigger. And so as a result, my  
1048 recommendation would be to have the default be noticed  
1049 because any definition that you use to come up with with harm  
1050 is going to be--it is probably going to be pretty flawed. It  
1051 is either going to be over-inclusive in which it would  
1052 include every single possibility of harm we can imagine, or  
1053 it is going to be under-inclusive and leave out huge chunks  
1054 of things that we want to protect against.

1055         And so as a result, my recommendation would be let us  
1056 not over-leverage the concept.

1057         Ms. {Schakowsky.} I know in the Sony breach we saw  
1058 employment records, for example, that were revealed. And so,  
1059 you know, that would be I think a problem for a lot of  
1060 people.

1061         So what about the--well, let me just put this on the  
1062 table, and maybe others would want to answer it at some other  
1063 point, the concern that there would be some sort of problem  
1064 of over-notification.

1065         Mr. {Hartzog.} The problem of over-notification is also  
1066 one that I think can tend to be over-inflated. So of course  
1067 you don't want consumers and people getting 45 emails a day

**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.**

1068 saying, oh, hey, guess what? You know, another piece of your  
1069 data has been breached. But I think we are a very long way  
1070 from reaching some kind of point where consumers would just  
1071 flippantly ignore some kind of piece of advice and--

1072 Ms. {Schakowsky.} I am going to go ahead actually and  
1073 cut you off because my time has expired, but I thank you.

1074 Mr. {Burgess.} The gentlelady yields back. The chair  
1075 now recognizes the Vice-Chair of the Full Committee, Ms.  
1076 Blackburn, 5 minutes for questions, please.

1077 Mrs. {Blackburn.} Thank you so much, Mr. Chairman. I  
1078 want to talk a little bit about doing a technology-neutral  
1079 data security requirement, and it seems like when we talk  
1080 about privacy, when we talk about data security, when we talk  
1081 about entertainment delivery, more and more we are hearing,  
1082 you know, don't get specific on the delivery system or don't  
1083 get specific on the technology because it takes us forever,  
1084 forever, to bring legislation into line with where technology  
1085 is.

1086 So we are going to start. Mr. Hartzog, I will start  
1087 with you. We will go all the way down the panel, and I just  
1088 want to hear your thoughts on technology-neutral or specific

**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.**

1089 and how you think we are best served to approach that.

1090 Mr. {Hartzog.} I would agree with you that we should  
1091 strive to be as technology-neutral as possible. We have seen  
1092 time and time again when we pass laws that are highly  
1093 technically specific that they are almost outdated the moment  
1094 they are passed. And so--

1095 Mrs. {Blackburn.} They are.

1096 Mr. {Hartzog.} --this is why things like reasonable  
1097 data security standards tend to make sense, and it also is  
1098 another good strong word of caution against really being  
1099 overly specific in any one particular area, and if to the  
1100 point where you have to be overly specific, being sure that  
1101 you have enabled the definition to change where possible. So  
1102 I would agree.

1103 Mrs. {Blackburn.} Okay.

1104 Ms. {Barrett-Glasgow.} I agree that the bill should be  
1105 technology-neutral. I think a good example of language  
1106 regarding security is the Gramm-Leach-Bliley security  
1107 provisions which have now stood the test of 15, 16 years or  
1108 so in the marketplace.

1109 And I would also, which actually may touch on Ms.

**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.**

1110 Schakowsky's question a little bit, in the Rush bill, H.R.  
1111 2221, the definition of harm reads determination that there  
1112 is no reasonable risk of identity theft, fraud, or other  
1113 unlawful conduct. And I think that other unlawful conduct  
1114 picks up a lot of opportunities as technology involves, as  
1115 new unlawfulness occur, for us to not have to come back and  
1116 revisit the language.

1117 Mrs. {Blackburn.} Got it.

1118 Mr. {Dodge.} So we would agree, of course, that we  
1119 should be technology-neutral. I don't think we can ever lose  
1120 sight of the fact that the criminals in this space are highly  
1121 sophisticated and rapidly evolving as we have seen in some of  
1122 the more recent reports, sometimes backed by nation states.  
1123 So allowing businesses to evolve as the threat evolves is  
1124 really important, and technology is a big part of that.

1125 Mrs. {Blackburn.} Okay.

1126 Ms. {Hyman.} And we would agree as well, technology-  
1127 neutral is an important principle. You know, we have gone  
1128 from simple redaction to encryption to more sophisticated  
1129 versions, and as has just been pointed out, you know, we have  
1130 to keep ahead of those that wish to cause harm. 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.**

1131 innovation of the private sector is a great opportunity to  
1132 lead on behalf of the consumers.

1133 Mrs. {Blackburn.} Okay. Thank you. Now, Ms. Hyman, we  
1134 are going to stay with you and come right back down the row.  
1135 When we are talking about preemption language, I want to  
1136 hear--and this is the lightning round. We have got a minute  
1137 and a half left on the clock. So what language do you want  
1138 to see us consider as we look at preemption?

1139 Ms. {Hyman.} Well, as I stated previously, we want to  
1140 make sure that we are not just ending up with the 48th  
1141 standard--

1142 Mrs. {Blackburn.} Okay.

1143 Ms. {Hyman.} --that it needs to be strong enough to  
1144 actually matter in terms of preemption and simplification.

1145 Mr. {Dodge.} A strong preemption sets a single,  
1146 national standard.

1147 Mrs. {Blackburn.} Okay.

1148 Mr. {Dodge.} Again, States deserve credit for the work  
1149 they have done, but you can't create a 48th law.

1150 Ms. {Barrett-Glasgow.} In my written testimony, I  
1151 actually suggested some language that you might want to take



**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.**

1152 a look at. I am not going to get into that right here.

1153 Mrs. {Blackburn.} Thank you.

1154 Mr. {Hartzog.} My recommendation would be preemption  
1155 that served as a floor but not a ceiling and at worst would  
1156 only preempt the very specific provisions listed by the  
1157 federal legislation.

1158 Mrs. {Blackburn.} Okay. Thank you all. I yield back.

1159 Mr. {Burgess.} The gentlelady yields back. The chair  
1160 now recognizes Ms. Clarke for 5 minutes for your questions,  
1161 please.

1162 Ms. {Clarke.} Thank you, Mr. Chairman, and I thank the  
1163 ranking member. I would like to drill down a bit more on the  
1164 breach notification issue.

1165 Breach notification laws and legislative proposals can  
1166 vary greatly in how they treat the question of when a company  
1167 affected by a breach is required to notify consumers. The  
1168 Data Accountability Trust Act, H.R. 2221, affirmatively  
1169 presumed a company affected by a breach would notify  
1170 consumers in the breach unless it determined that there is a  
1171 reasonable risk of identity theft, fraud, and other unlawful  
1172 conduct. There have also been proposals with a ``negative

**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.**

1173 presumption,' in other words, that a company does not have  
1174 to notify consumers unless an investigation reveals that a  
1175 certain level of risk exists to the consumers whose  
1176 information was breached. The burden to prove risk in this  
1177 case is not on the breached holder of consumers' personal  
1178 information but rather on those challenging its breach  
1179 notification practices.

1180           So Professor Hartzog, have you thought through what  
1181 should be the presumption for firms to notify consumers of a  
1182 breach and if so, why?

1183           Mr. {Hartzog.} Thank you very much. I have, and my  
1184 recommendation would be to a presumption of notification in  
1185 terms of breach. There are some interesting options  
1186 available with respect to granting a safe harbor that are  
1187 still debatable. Maybe if you make information unusable,  
1188 unreadable, using things like encryption standards, then that  
1189 is something that States have been experimenting with. That  
1190 is a positive element, although that is not free from  
1191 controversy with respect to the effectiveness of encryption.  
1192 But when the presumption is that you don't have to notify  
1193 unless an assessment of risk of harm proves that 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.**

1194 likely, then you miss out on a great deal of notifications.  
1195 And it is important to remember that notifications are  
1196 important not just for the individual that is being notified  
1197 but also for other companies that are similarly situated so  
1198 that they can know about threats that are facing them and  
1199 perhaps practically respond to them, for State AGs, for the  
1200 public so that they can be aware, just become more aware of  
1201 the issues about data breach generally speaking.

1202           So when the default is set and a practical effect will  
1203 result in far fewer notifications, then I think that the  
1204 public and other companies that--and individuals are--

1205           Ms. {Clarke.} So that brings me back around to the  
1206 question raised by Ranking Member Schakowsky. She broached  
1207 this issue of over-notification with you, and one of the  
1208 concerns raised about breach notification is notification  
1209 fatigue or over-notification. Would a negative presumption  
1210 for notification be effective in preventing over-  
1211 notification?

1212           Mr. {Hartzog.} I think that it is not so much as to  
1213 whether the presumption of harm trigger would be effective in  
1214 preventing over-notification. Certainly it would probably

**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.**

1215 result in fewer notifications. So then the question becomes  
1216 is that a good thing or a bad thing? And I again state that  
1217 we collectively lose out when notifications drop, even though  
1218 there have been breaches because there is value we can get  
1219 from notification. And also, over-notification is a problem  
1220 not just aided by reduction in notification, but we also need  
1221 to continue to experiment with the way notification is given.  
1222 There is a presumption maybe that notification is just a big  
1223 dense block of text that individuals would--it is very easy  
1224 just to look at and throw in the trash. One of the reasons  
1225 we still need to experiment, perhaps at the State law level,  
1226 is that we need to focus on the way notification is actually  
1227 delivered because there is a lot of opportunity there to  
1228 avoid oversaturation as well.

1229 Ms. {Clarke.} Did any of you want to weigh in on the  
1230 issue of over-notification or concerns that your industries  
1231 may have? Ms. Glasgow?

1232 Ms. {Barrett-Glasgow.} Yes. I will go back to H.R.  
1233 2221, and the language that is in there I think is reasonable  
1234 and good in terms of both the risk of harm as well as the  
1235 presumption of notification unless it says the person shall

**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.**

1236 be exempt from the requirement, meaning the notification, if  
1237 certain conditions apply.

1238 I think we have to be very careful about over-  
1239 notification. I think we have learned through not just  
1240 breach notification laws that exist today but also other  
1241 requirements such as Gramm-Leach-Bliley privacy notices that  
1242 when consumers get repeated information about risks or about  
1243 even what a bank may do with their data and there is no clear  
1244 instruction as to what to do, and there may not be any  
1245 recourse other than watch your accounts, that is possible,  
1246 then they tend to get far more complacent about them and  
1247 potentially even not read the one that really was the one  
1248 that they needed to react and respond to. So I think  
1249 industry in general is very sensitive to the over-  
1250 notification problem.

1251 Ms. {Clarke.} Let me just say very quickly in closing,  
1252 is there something that we can learn? Is there value to  
1253 proceeding with notifications simply in terms of uncovering  
1254 what works best? We are really in the advent of  
1255 understanding exactly what is taking place. We wanted to get  
1256 a sense of whether in fact there is value. Mr. Hartzog?

**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.**

1257           Mr. {Hartzog.} One of the great benefits of breach  
1258 notification statutes is it allows us to collect information  
1259 and then issue reports which could then benefit not only  
1260 companies but the field of data security generally because it  
1261 helps us know where threats are coming from, what the  
1262 response to those threats are, and how long it takes to  
1263 respond.

1264           Mr. {Burgess.} The gentlelady's time has expired. The  
1265 chair thanks the gentlelady. The chair now recognizes the  
1266 Vice-Chair of the Subcommittee, Mr. Lance, for 5 minutes for  
1267 questions, please.

1268           Mr. {Lance.} Thank you, Mr. Chairman. This is a very  
1269 complicated issue, and we don't want to become the 48th and  
1270 yet we want strong protection. And I think it is going to be  
1271 a difficult needle to thread.

1272           Ms. Glasgow, as I understand your testimony, you believe  
1273 that we threaded the needle relatively well in Gramm-Leach-  
1274 Bliley, is that accurate?

1275           Ms. {Barrett-Glasgow.} As in regards to the security  
1276 rule, yes.

1277           Mr. {Lance.} Yes. And do other distinguished members

**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.**

1278 of the panel have an opinion on that and how it might relate  
1279 to what we are attempting to do here? Ms. Hyman?

1280 Ms. {Hyman.} As we think about harm and the risk of  
1281 over-notification and how we should be looking at this, we  
1282 want to make sure that the information that is exposed  
1283 actually is significant harm. So just having for example a  
1284 name or address on its own without other identifiable  
1285 information like a Social Security, these things need to be  
1286 seen in context, and how we thread that will be important.

1287 Mr. {Lance.} Mr. Dodge?

1288 Mr. {Dodge.} So I think the regulatory regimes that  
1289 cover businesses should reflect the businesses themselves,  
1290 but specific to notification, I believe that consumers should  
1291 have a strong expectation of how they would be notified if  
1292 certain information, personally identifiable information, is  
1293 lost regardless of the business itself. It should be based  
1294 on the data.

1295 Mr. {Lance.} Professor Hartzog?

1296 Mr. {Hartzog.} I think the Gramm-Leach-Bliley  
1297 safeguards protections have been quite effective. They are  
1298 technology-neutral and recognize data security as a process

**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.**

1299 rather than just a one-time thing. So I would say that that  
1300 has been very effective.

1301 Mr. {Lance.} So this might be an area of agreement in  
1302 the panel, and I think this subcommittee and then the Full  
1303 Committee want to reach a point where we can report to the  
1304 Floor a bipartisan bill that moves the Nation forward.

1305 It has been a long time since I went to law school, but  
1306 do we look ultimately to fundamental principles of tort law,  
1307 Professor Hartzog, as to what we should be doing here?

1308 Mr. {Hartzog.} I would caution against relying on tort  
1309 law too heavily, mainly because tort law is entrenched in a  
1310 harm-based mindset.

1311 Mr. {Lance.} That is why I asked the question.

1312 Mr. {Hartzog.} And we see that because of causation  
1313 issues, because it is very difficult to prove that one piece  
1314 of notification when compromised results in some kind of  
1315 tangible harm on the other end--I teach tort law, and  
1316 causation is one of the things you always end up getting  
1317 tripped up on. And so I would actually caution away against  
1318 looking to tort law and look into more general proactive  
1319 regulatory principles.



**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.**

1320 Mr. {Lance.} I was taught tort law by John Wade who is  
1321 the reporter of the restatement in the law school not too far  
1322 from where you teach, just a little north of where you teach.  
1323 How about others on the panel regarding should we look at all  
1324 to tort law or is it not broad enough given our desire in a  
1325 bipartisan fashion to protect the public. Mr. Dodge?

1326 Mr. {Dodge.} I know when I am out over my skis, so I  
1327 wouldn't--

1328 Mr. {Lance.} I see.

1329 Mr. {Dodge.} --be able to comment on that.

1330 Mr. {Lance.} I see. Ms. Glasgow?

1331 Ms. {Barrett-Glasgow.} No, I am a technologist, not a  
1332 lawyer so--

1333 Mr. {Lance.} Okay. That speaks well of you. Ms.  
1334 Hyman?

1335 Ms. {Hyman.} Unfortunately, I have to join my  
1336 colleagues on that.

1337 Mr. {Lance.} I see. I won't take all of my time, but  
1338 let me say that the chairman and I have discussed this at  
1339 some length, and we want to be able to report a bipartisan  
1340 bill. But we don't want this to be the 48th state. We want

**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.**

1341 to move the Nation forward, and we want strong consumer  
1342 protection. And I know the chairman is dedicated to that as  
1343 am I, and I hope that we can all work together. And I see  
1344 some areas of agreement. Thank you, Mr. Chairman.

1345 Mr. {Burgess.} The chair thanks the gentleman. The  
1346 gentleman yields back. The chair recognizes the gentleman  
1347 from Massachusetts, Mr. Kennedy, 5 minutes for your  
1348 questions, please.

1349 Mr. {Kennedy.} Thank you, Mr. Chairman. Thank you to  
1350 the witnesses for testifying today. Insightful hearing. I  
1351 want to build off actually some of the comments that my  
1352 colleague, Mr. Lance, just talked about and touched on and  
1353 try to see if we can thread that needle a little bit.

1354 As he indicated, 47 States, the District of Columbia,  
1355 Guam, Puerto Rico, and the Virgin Islands have all enacted  
1356 their own laws requiring notification of security breaches  
1357 involving personal information. Some States, such as  
1358 Massachusetts and California, have mandated strong  
1359 requirements. California's data breach notification law  
1360 requires that a person be notified when their encrypted  
1361 personal information has been or is reasonably believed 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.**

1362 have been acquired by an unauthorized person, and the  
1363 consumer has the right to know about all breaches of personal  
1364 information, not just those deemed capable of doing harm.

1365           Massachusetts law mandates that data owners provide  
1366 notice of a security breach to the State's Consumer Affairs  
1367 Office, State Attorney General, and the affected resident and  
1368 include any steps the data-holder has taken relating to the  
1369 incident.

1370           Professor Hartzog, some legislative proposals include  
1371 preemption of ``any provision of a law, rule, regulation,  
1372 requirement, standard, or other provision having force and  
1373 effect of law relating to either data security of personally  
1374 identifiable information or notification following a breach  
1375 of personal, identifiable information.'' As I understand it,  
1376 that would not be limited to the 47 States' statutes but it  
1377 could, building off of a comment a moment ago, also preempt  
1378 tort law and contract law. Seeing as you are a tort  
1379 professor, is that correct and can you just walk us through  
1380 that a little bit?

1381           Mr. {Hartzog.} Sure. So that strikes me as very broad  
1382 preemptive language and the kind of which I would recommend

**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.**

1383 against, precisely because while tort law isn't our best  
1384 hope, we still might actually find some hope in tort law,  
1385 maybe not in the tort of negligence which is very harm based,  
1386 but perhaps other theories. So some of the more successful  
1387 theories at the State level with regard to data security have  
1388 been promises made by companies about data security which is  
1389 sort of a tort and contract mixture. And for legislation to  
1390 preempt that I think would be very problematic, and I think  
1391 we have to be very careful about broad preemption with  
1392 respect to federal sector-specific data security law as well  
1393 because there are some extremely important protections that  
1394 exist throughout in various different sectors.

1395 And so that kind of preemptive language is exactly the  
1396 kind of preemptive language that would strike me as one that  
1397 would ultimately end up doing more harm than good based on  
1398 how significant it would seem to scale back protections for  
1399 consumers.

1400 Mr. {Kennedy.} So building off of that, Professor, as I  
1401 understand it, Massachusetts data breach law has some strong  
1402 data security requirements which include the authority of the  
1403 Massachusetts Department of Consumer Affairs and Business

**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.**

1404 Regulation to issue regulations regarding data security.  
1405 Would those regulations then be preempted potentially by that  
1406 language that I just referenced? We obviously, yes, don't  
1407 want to add in another layer of regulation but want to make  
1408 sure that there is some strong consumer protection standards  
1409 and allow States to innovate here as well.

1410 Mr. {Hartzog.} That is correct. That language would  
1411 seem to preempt the State law protections in Massachusetts as  
1412 well as all the other States that have data security  
1413 requirements related to it, and this is potentially  
1414 problematic because while the general approach to regulating  
1415 data security seems relatively consistent--we all want  
1416 reasonable data security practices which is relatively  
1417 tethered to industry standards--States and policymakers in  
1418 general are still trying to figure out exactly the best  
1419 approach to that. And it would seem to be a problem to set  
1420 something in stone when we are still trying to grapple with  
1421 this very important issue.

1422 Mr. {Kennedy.} Okay. Thank you, Professor. I will  
1423 yield back.

1424 Mr. {Burgess.} The gentleman yields back. The chair

**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.**

1425 recognizes the gentleman from Mississippi, Mr. Harper, 5  
1426 minutes for your questions, please.

1427 Mr. {Harper.} Thank you, Mr. Chairman, and thanks to  
1428 each of you for being here. It is a great concern as to how  
1429 you protect the consumers and reduce the burden here and  
1430 maybe prosecute the bad guys. So there is a lot to be done.  
1431 This affects--I don't know of a company that is not greatly  
1432 impacted and truly troubled by this.

1433 First question would be a follow-up, Mr. Dodge. Some  
1434 have suggested that consumers should receive notice from the  
1435 company that was breached, even if they have never interacted  
1436 with that company. Wouldn't it be clear for a consumer if  
1437 they receive notification about a breach from the company  
1438 that they actually gave the information to directly?

1439 Mr. {Dodge.} So we think that the obligation to notify  
1440 creates a very important incentive to keep systems strong and  
1441 protect the information that companies hold. We would urge  
1442 the committee as it considers this to maintain that  
1443 obligation but allow for flexibility for businesses to  
1444 contractually determine the notifying party because I think  
1445 there are situations that you describe where that 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.**

1446 appropriate. But to try to contemplate all those situations  
1447 would be problematic and could undermine that important  
1448 incentive.

1449 Mr. {Harper.} Is there a risk to consumers that you  
1450 could create some confusion by duplicate notification from  
1451 the company they gave information to and also a third party?  
1452 What do you say about that?

1453 Mr. {Dodge.} So again, I think the objective from all  
1454 the parties involved would be to make sure that it was a  
1455 streamlined and clear notification. And so that is why we  
1456 would argue that the value of maintaining that incentive is  
1457 high, but allowing flexibility for the parties involved as  
1458 you described to contractually determine who would distribute  
1459 that notice.

1460 Mr. {Harper.} And this would be a question to Ms.  
1461 Hyman, you, Mr. Dodge, and Ms. Glasgow. Some States trigger  
1462 notification to individuals after the company determines that  
1463 there has been an unauthorized access to their information  
1464 while the majority of States require notice upon a reasonable  
1465 belief that the data was acquired by an unauthorized party.  
1466 So the data was actually removed from the system. Is there 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.**

1467 danger of over-notification to consumers if the duty to  
1468 notify individuals is triggered by access but not  
1469 acquisition?

1470 Ms. {Hyman.} Yes, there is, and we think it is very  
1471 important that companies have an opportunity to do an  
1472 appropriate risk assessment to determine whether there has  
1473 been actual access to the information.

1474 Mr. {Harper.} Mr. Dodge?

1475 Mr. {Dodge.} We believe that it has to be at the time  
1476 of the confirmed breach. You want to be able to, in the wake  
1477 of a breach, to define the universe of affected individuals  
1478 so that the notice goes to the people who truly were or could  
1479 be impacted, rather than overly broad and catching people  
1480 that perhaps weren't affected.

1481 Mr. {Harper.} Okay. Ms. Glasgow?

1482 Ms. {Barrett-Glasgow.} You know, the subtle difference  
1483 between access and acquisition is really kind of lost I think  
1484 in this debate in that if there is access and it is from an  
1485 unauthorized person, you more than likely have some potential  
1486 risk.

1487 So if a company is assessing that, I think responsible



**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.**

1488 companies are going to err on the side of caution.

1489 Mr. {Harper.} And Ms. Glasgow, earlier you testified  
1490 when we were talking about a national notification standard,  
1491 you mentioned a harm-based standard. Who is going to  
1492 determine--in your eyes, who is best able to determine if  
1493 there is harm?

1494 Ms. {Barrett-Glasgow.} Well, I think it is determined  
1495 by a number of parties. First, the company is the one that  
1496 is on the line to begin with to make that assessment based on  
1497 their understanding of what has happened. But beyond that,  
1498 there are various regulatory agencies, the FTC at the federal  
1499 level and of course State AGs at the State level, that put  
1500 teeth into that analysis to make sure that that assessment is  
1501 done effectively and fairly for all parties.

1502 Mr. {Harper.} Just as a comment. When you have 47  
1503 standards and you have a company, most companies are national  
1504 companies. It is extremely confusing and difficult for them,  
1505 and that is why as we look toward a bipartisan approach to  
1506 this, it is going to be very important how we move forward.

1507 Mr. Dodge, if I could ask you, while there are ongoing  
1508 discussions on how to establish a sensible time period 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.**

1509 which companies are required to notify consumers of a breach,  
1510 I am also interested in understanding what exactly or who  
1511 exactly would start the notification timeframe so there is no  
1512 room for misinterpretation of when companies are required to  
1513 notify consumers. I would imagine that your members would  
1514 not want this left up for interpretation after the fact.  
1515 What are your thoughts on when this clock should start and  
1516 who should be responsible for starting it?

1517 Mr. {Dodge.} So we believe that the trigger should be  
1518 the confirmation of a breach, and at that point of course  
1519 there are lots of players who would be involved from law  
1520 enforcement to presumably regulators if Congress were to go  
1521 down this path. I think what is important to remember that  
1522 there needs to be flexibility in that timeline because there  
1523 are a number of steps that need to occur in order to ensure  
1524 that the notice that goes out provides actionable  
1525 information. So you want to first define the universe as I  
1526 said a moment ago. Then you need to train your staff because  
1527 invariably when these notices are received, it is going to  
1528 lead to a number of questions. It won't be limited to the  
1529 phone number or whatever the method of contact is on 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.**

1530 notice. So you need to train staff in order to be able to  
1531 respond and help consumers protect themselves.

1532 And then there is the complex process of sending out a  
1533 notice. It could be extremely large scale and making sure  
1534 that notices aren't just going into junk mailboxes.

1535 Mr. {Harper.} And not meaning to cut you off, my time  
1536 is expired. Thank you, Mr. Chairman.

1537 Mr. {Burgess.} The gentlelady yields back. The chair  
1538 thanks the gentleman. The chair now recognizes the gentleman  
1539 from Vermont, 5 minutes for your questions, please.

1540 Mr. {Welch.} Thank you. I didn't know whether Mr. Rush  
1541 was ahead of me or not, but he tells me he is not from  
1542 Vermont. So I am okay to go. We would love to have you.

1543 Thank you very much. This is extremely helpful. A  
1544 couple of the issues we are wrestling with is, number one, is  
1545 preemption, and in general, I favor non-preemption but I have  
1546 been persuaded that if we can get the right standard, this is  
1547 one of those situations where it really makes sense to have  
1548 preemption.

1549 Let me just go down the line like my colleague, Marsha  
1550 Blackburn, did. If we have preemption, it is going to give 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.**

1551 think a lot more comfort to those of us who are willing to  
1552 take that step if the standard is stronger, and we have got a  
1553 strong standard in Illinois. We have got a strong standard  
1554 in California. In my conversations with some folks in the  
1555 industry, the advantage of a single standard makes them  
1556 supportive of a strong standard. And I want to just get each  
1557 of your views on that. In other words, if we have  
1558 preemption, do you support a relatively robust standard?

1559 Ms. {Hyman.} We have spoken out in favor of significant  
1560 harm to the consumer. States are justifiably proud of the  
1561 work that they have done. The chairman of our IT security  
1562 group is from Massachusetts, but he, too, has shared with us  
1563 the notion that the patchwork has become unworkable--

1564 Mr. {Welch.} Right. So--

1565 Ms. {Hyman.} --for companies such as theirs. So--

1566 Mr. {Welch.} --you get a single standard, a strong  
1567 standard is something you could support if you got  
1568 preemption?

1569 Ms. {Hyman.} Yes.

1570 Mr. {Welch.} And how about you, Mr. Dodge?

1571 Mr. {Dodge.} Again, based on the recognition in 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.**

1572 case of harm or risk to consumers, yes, we totally agree, and  
1573 we believe that the preemption is really, really critical.

1574 Mr. {Welch.} Okay. Thank you. Ms. Glasgow?

1575 Ms. {Barrett-Glasgow.} Yes, the harm-based trigger tied  
1576 with federal preemption is very acceptable.

1577 Mr. {Welch.} Okay. And Mr. Hartzog?

1578 Mr. {Hartzog.} Well, I would say that if federal  
1579 legislation is really going to move the ball forward and not  
1580 actually strip away existing protections, then we should not  
1581 have a harm-based trigger, and we should also, even to the  
1582 extent that we should have broad definitions of things like  
1583 PII which we have now, that may actually change in the  
1584 future. And so we need to be sure that we can change the  
1585 law--

1586 Mr. {Welch.} If I understood your testimony, though,  
1587 you had reservations about preemption, but you weren't  
1588 categorically opposed to it.

1589 Mr. {Hartzog.} That is correct. That is right.

1590 Mr. {Welch.} Your concern is that whatever our standard  
1591 is, it be robust.

1592 Mr. {Hartzog.} That is right.

**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.**

1593 Mr. {Welch.} Correct?

1594 Mr. {Hartzog.} So, so long as the standard is at or  
1595 above what we currently have now, then I think that we can  
1596 continue to move in the correct trajectory for data breach.

1597 Mr. {Welch.} Okay. Thank you for that. The other  
1598 question is if you have a single standard, can you have that  
1599 be enforceable at the local Attorney General level as well as  
1600 at the federal level? And folks like Illinois, the Attorney  
1601 General has been very active in this. I know Vermont has  
1602 been active in local enforcement. Would there be any problem  
1603 with allowing the enforcement of that standard, both at the  
1604 federal and at the state level, where people would have I  
1605 think more confidence that they would be heard? Let us go  
1606 down the line.

1607 Ms. {Hyman.} Sure. We understand and accept the notion  
1608 that the State Attorneys General should have the opportunity  
1609 to enforce or the FTC or the federal body, but we would argue  
1610 that one should extinguish the other. In other words, you  
1611 shouldn't have those contemporaneously.

1612 Mr. {Welch.} I see. Okay. Mr. Dodge?

1613 Mr. {Dodge.} Just building off that, I think we do

**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.**

1614 recognize that there is an important role for the State AGs  
1615 to play in this.

1616 Mr. {Welch.} Thank you.

1617 Ms. {Barrett-Glasgow.} Yeah, I agree, and so long as  
1618 the coordination between State AGs and FTC is in place.

1619 Mr. {Welch.} Okay. Mr. Hyman [sic]?

1620 Mr. {Hartzog.} I would agree that enforcement of the  
1621 State AGs would be desirable for a data breach.

1622 Mr. {Welch.} Okay. The other question I want to go to  
1623 is this whole issue of tort law, and I understand that is  
1624 somewhat injected into this. My understanding is, and  
1625 correct me if I am wrong, the issue of tort law just applies  
1626 in general across commerce and across non-commercial  
1627 activity, and this committee, I am not sure--Mr. Chairman, I  
1628 thought you were correct in your opening statement for  
1629 acknowledging in some areas we simply don't have the  
1630 jurisdiction to get involved. And I am thinking--

1631 Mr. {Burgess.} Would the gentleman yield?

1632 Mr. {Welch.} Yes, I will.

1633 Mr. {Burgess.} For his purposes going forward, the  
1634 chair is always 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.**

1635           Mr. {Welch.} That more or less settles it. But I see  
1636 that this whole question of tort law and whether there should  
1637 be some carve-out as really a separate question from the  
1638 heart of this legislation. There are a lot of folks that  
1639 would love to not ever have to worry about tort law, but that  
1640 is across the whole spectrum of any kind of activity in  
1641 society, and taking that challenge on in this legislation may  
1642 be a burden that is inappropriate to bear and too great to  
1643 bear.

1644           So I just want to get your comment as to whether some  
1645 tort provision in here in your mind is essential to getting  
1646 some of the good things that both sides seem to be  
1647 supporting.

1648           Ms. {Hyman.} Well, again, I will point out I am  
1649 recovering lawyer. So my familiarity with tort law is a  
1650 little bit obscured at this point in time. But the one thing  
1651 I would say is that we need to separate out and distinguish  
1652 between good actors and bad actors. And what this effort  
1653 about data breach notification is about is trying to provide  
1654 clear lines of responsibility between the companies and the  
1655 consumer. There are always going to be people that are bad



**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.**

1656 actors, and they should be punished.

1657 Mr. {Welch.} Right.

1658 Ms. {Hyman.} That is a different subject.

1659 Mr. {Welch.} Okay. Mr. Dodge?

1660 Mr. {Dodge.} I, too, am not a lawyer, so I can't speak  
1661 to the details of tort law. But I would say that, you know,  
1662 this whole exercise is about empowering customers, consumers,  
1663 with expectations around how they would receive notice and  
1664 empowering businesses to conform to a standard.

1665 Mr. {Welch.} All right. I see my time is expired. So  
1666 the last two dodged the bullet. Thank you. I yield back.

1667 Mr. {Burgess.} The chair thanks the gentleman. The  
1668 chair now recognizes the gentleman from Texas, Mr. Olson, 5  
1669 minutes for your questions, please.

1670 Mr. {Olson.} Thank you, Mr. Chairman, and  
1671 congratulations on your first hearing of this important  
1672 subcommittee, and welcome to all of our witnesses. I assure  
1673 you, I went to law school, but you won't hear the word tort  
1674 come out of my mouth through my questions.

1675 Unfortunately, in today's world, data breaches are  
1676 happening more and more often. Target, Home Depot, Neiman

**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.**

1677 Marcus, Sony Pictures all have been attacked by very  
1678 different bad actors. We have to be aggressive on account of  
1679 this threat, but it is a bit but, we must craft a balanced  
1680 approach that protects consumers without undue burdens upon  
1681 business.

1682 My first line of question is about notification. I want  
1683 to bore down the issue a little bit. My first question to  
1684 you, Ms. Hyman, is it realistic to require any company to  
1685 notify consumers within a set number of days after a breach  
1686 occurs?

1687 Ms. {Hyman.} Thank you, Congressman. First of all, I  
1688 just want to reiterate, businesses are incented to be  
1689 responsible to the consumer. This is about trying to make  
1690 sure that the consumer has information quickly and it is  
1691 actionable.

1692 There needs to be a reasonable period of time to do a  
1693 risk assessment to find out, as was pointed out by my  
1694 colleague, was there actual harm? You know, are there  
1695 opportunities to remedy that harm? What kind of messaging is  
1696 being provided to the workforce so that they can respond to  
1697 the consumer when a notice goes out? So a reasonable period

**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.**

1698 of time needs to be in place for risk assessment.

1699 Thereafter, if there is an appropriate timeframe for the

1700 actual notification, that makes a lot of sense.

1701 Mr. {Olson.} How about if they have some notification,  
1702 when did this breach occur? Wouldn't we say that is where it  
1703 happened, that is where the notification period starts? I  
1704 mean, I am so confused when this clock starts running. Any  
1705 idea when that clock starts running, ma'am?

1706 Ms. {Hyman.} I think you are saying does the clock  
1707 start--

1708 Mr. {Olson.} Yeah, when does it start? You said it is  
1709 reasonable.

1710 Ms. {Hyman.} When there is an actual breach.

1711 Mr. {Olson.} Okay. When does it start if it is  
1712 reasonable? When do we start the clock? When has the breach  
1713 occurred?

1714 Ms. {Hyman.} As soon as there is any type of  
1715 information for the company to take a look and do the risk  
1716 assessment, they have to do that within a reasonable period  
1717 of time.

1718 Mr. {Olson.} Okay. Mr. Dodge, how about you, sir? How

**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.**

1719 about--is there reasonable required notification within a set  
1720 number of days?

1721 Mr. {Dodge.} So we would urge flexibility in  
1722 determining what that length of time is. As we have talked  
1723 about, there are a number of steps that need to occur. But  
1724 in every instance, the business entity that I am aware of has  
1725 a desire to communicate that quickly because they want to  
1726 make sure they are limiting any exposure or risk to those  
1727 affected by the breach itself.

1728 Mr. {Olson.} Ms. Glasgow, I know you are a UT Longhorn  
1729 and probably want to talk about this issue. Any concerns  
1730 about requiring notification of breaches?

1731 Ms. {Barrett-Glasgow.} Yes. I think there are two.  
1732 First, any kind of deadline tends to become the norm so that--  
1733 --and some breaches are very simple or small breach,  
1734 notification can take place in a matter of days or weeks if  
1735 it is contained, a briefcase that is lost or something that  
1736 is easily to investigate.

1737 A big, complicated breach like we saw with some of the  
1738 recent ones that you mentioned, take much longer. And so,  
1739 you know, we run the risk of extending a simple breach to 30

**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.**

1740 days because that is the rule. But we also run the risk of  
1741 not having enough information to do the assessment. And so--  
1742 and the notification process may be iterative. Through an  
1743 investigation, you don't always have all the facts  
1744 immediately. I mean, think about any criminal investigation  
1745 that law enforcement takes. You learn something, and from  
1746 that you ask more questions and from that you ask more  
1747 questions. So it can very much be an interactive process of  
1748 learning over a fairly extended period of time. So I think  
1749 any kind of arbitrary number is inappropriate.

1750         You know, language like we suggested in our written  
1751 testimony that says without undue delay we think creates the  
1752 sense of urgency but doesn't necessarily penalize the very  
1753 complicated investigation.

1754         Mr. {Olson.} And one final question about harmless  
1755 breaches. We all agree that there are breaches that are  
1756 harmless, yes or no? Ms. Hyman, yes or no, harmless  
1757 breaches? We agree that some breaches are harmless?

1758         Ms. {Hyman.} Yes, there are some harmless breaches  
1759 because of the type of information that is accessed.

1760         Mr. {Olson.} Mr. Dodge?

**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.**

1761 Mr. {Dodge.} Yes, of course there are situations where  
1762 intrusions can occur and no information has been taken.

1763 Mr. {Olson.} Ms. Glasgow?

1764 Ms. {Barrett-Glasgow.} Yes. I will give another  
1765 example and that is when the information that was taken is  
1766 encrypted or is essentially in some form that is unusable by  
1767 the thief.

1768 Mr. {Olson.} And Mr. Hartzog, Professor Hartzog?

1769 Mr. {Hartzog.} I would say it depended on how you  
1770 define harm. There are lots of different ways to think about  
1771 it. I mean, does it result in--was the breach a result of  
1772 poor security practices, even though it didn't result in  
1773 financial harm? It resulted in perhaps a breach of trust.  
1774 Even if it is rendered unusable, if the encryption standard--  
1775 was it adequate to actually protect the data? And so I would  
1776 actually hesitate from saying yes to that question simply  
1777 because the way you define harm is everything and that--

1778 Mr. {Olson.} With you leaning yes, sir. I yield back.

1779 Mr. {Burgess.} The gentleman yields back. The chair  
1780 thanks the gentleman. The chair now recognizes the former  
1781 chairman of the subcommittee, my longtime friend, Bobby Rush,

**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.**

1782 from Chicago.

1783 Mr. {Rush.} Thank you. Thank you, Mr. Chairman, and I  
1784 want to also congratulate you on your first hearing. It is  
1785 an outstanding hearing, and I want to congratulate all your  
1786 witnesses. They have provided fine testimony. And Mr.  
1787 Chairman, I am going to take your pronouncement under  
1788 consideration that you are always right, that you are never  
1789 wrong--no, you said you are always right. And I am going to  
1790 really try to process that because I am never wrong. So we  
1791 have come to some kind of mutual understanding and agreement  
1792 on that, all right?

1793 Mr. Chairman, I want to get to the matter of the day,  
1794 and I want to talk Dr. Hartzog. Dr. Hartzog, I am of the  
1795 opinion that somebody has got to be in charge of  
1796 interpretation. Somebody has got to be in charge of  
1797 implementation, all right? And I understand you call for  
1798 regulation by multiple agencies in their areas of expertise.  
1799 Beauty is in the eye of the beholder, and one of the issues  
1800 that we are always struggling with in this place is who has  
1801 got the final say? Who has got jurisdiction and what is it  
1802 that they have jurisdiction over?

**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.**

1803           My question to you is, first of all, if you can kind of  
1804 explain to us and clarify what do you mean by regulation by  
1805 multiple agencies in their areas of expertise? Can you be a  
1806 little bit more clear in regards to that? And my second  
1807 question is do you believe that there should be one central  
1808 agency who could be the final authority on data security for  
1809 the Federal Government?

1810           So will you try and clarify your perceptions in terms of  
1811 jurisdictional issues?

1812           Mr. {Hartzog.} Sure. So thank you for the question. I  
1813 think that there should not be one entity that is in charge  
1814 of data security for the entire country simply because data  
1815 security is--what constitutes good data security and  
1816 reasonable data security is so highly dependent upon context  
1817 and industry. And so we have already existing numerous  
1818 regulatory agencies, like the Federal Communications  
1819 Commission, HHS and HTSA, the FAA, many different regulatory  
1820 agencies, all of which have in some form spoken and made some  
1821 requirements for good data security or looking into  
1822 requirements for data security. And it is imperative that we  
1823 rely upon these multiple regulatory bodies because they 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.**

1824 expertise in very specific things. So the Federal  
1825 Communications Commission has well-developed expertise in  
1826 regulating telecommunications companies, satellite companies,  
1827 and cable companies and other intermediaries and the specific  
1828 data security requirements that apply in those particular  
1829 fields, which might differ than say a standard commercial  
1830 enterprise.

1831 That being said, sometimes there is overlapping  
1832 jurisdiction, but what we have seen with multiple regulatory  
1833 agencies is we have seen that they can coexist. They work  
1834 together. Sometimes they have coordinated investigations.  
1835 Sometimes they reach memorandums of understanding where they  
1836 say, you know, you will handle certain kinds of data security  
1837 breaches, and we will handle other kinds.

1838 And so that is what I meant by the importance of  
1839 regulatory bodies, multiple regulatory bodies.

1840 Mr. {Rush.} I have a second question here, and this is  
1841 directed to Ms. Glasgow. The Federal Trade Commission called  
1842 on Congress to enact the legislation to allow consumers with  
1843 access to information held by data brokers. The Commission  
1844 has also recommended that one centralized Web site be created

**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.**

1845 where consumers can learn about how their data is used,  
1846 correction to inaccuracies of their data, and to opt out for  
1847 marketing if desired. Do you support these recommendations?

1848 Ms. {Barrett-Glasgow.} We actually have gone so far as  
1849 to implement the recommendation to have one central site  
1850 where clients can come and look--or consumers, excuse me, can  
1851 come and look at the data that Acxiom holds and correct it  
1852 and change it. And we continue to work with industry on  
1853 whether or not having a central site where everyone lists  
1854 themselves and a consumer goes there, how that might be  
1855 effective in terms of transparency. We certainly support the  
1856 objective that the FTC has stated relative to transparency.

1857 Mr. {Rush.} I only have a few seconds, but can you  
1858 share with the committee some of your experiences? I mean,  
1859 how do the consumers, how do they go about it? How do they  
1860 grade their experience with Acxiom?

1861 Ms. {Barrett-Glasgow.} Yes. The site requires the  
1862 consumer to log in and identify themselves because we are  
1863 going to be sharing the data that we have about them on that  
1864 site. So we have to know who they are, but once they have  
1865 logged in and established an account, then they can look at

**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.**

1866 all the data that we used for any of our marketing products.  
1867 They can delete an element. They can change an element, or  
1868 they can completely opt out of the whole process online, and  
1869 it happens in real time. We would encourage you to maybe go  
1870 to the site and take a look. It is called AboutTheData.com.

1871 Mr. {Rush.} Thank you, Mr. Chairman. I yield back.

1872 Mr. {Burgess.} The chair thanks the gentleman. The  
1873 gentleman yields back. The chair now recognizes the  
1874 gentleman from Florida, Mr. Bilirakis, 5 minutes for your  
1875 questions.

1876 Mr. {Bilirakis.} Thank you, Mr. Chairman. I appreciate  
1877 it very much, and again, thanks for holding this very  
1878 important hearing, and I really thank the panel as well.  
1879 This is so important to our consumers.

1880 Consumers must be able to trust that information they  
1881 provide. They want to make sure that it is safe. They  
1882 provide the information to retailers, and the digital world  
1883 where sales are increasing on line, such as--you know, this  
1884 trust is vital to our economy. However, I do not believe  
1885 such trust will be preserved by the current patchwork of  
1886 laws. We need a stable law that ensures merchants are

**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.**

1887 appropriately protecting consumers without sacrificing  
1888 prosperity.

1889           The first question is for Mr. Dodge. You mentioned in  
1890 your testimony the benefits of the chip and PIN that we are  
1891 transitioning to nationwide. However, my understanding is  
1892 that a potential weakness exists for online transactions  
1893 because the payment card is not actually present. Doesn't  
1894 that mean that this technology and every other technology can  
1895 be made obsolete by criminals that quickly adapt to new  
1896 technologies? It seems to me that we need to ensure that  
1897 what we pass into law meets the threat and is not  
1898 prescriptive of one type of technology? Do you agree and  
1899 what do you recommend?

1900           Mr. {Dodge.} So just a couple of points first,  
1901 specifically chip and PIN is not scheduled to be rolled out  
1902 later this year. This has been a major point of tension  
1903 between the merchant community and the financial services  
1904 community because the expectation is the chip only is coming  
1905 out. Chip and PIN has been in place around the world for  
1906 many, many years and has been proven to dramatically reduce  
1907 fraud. Retailers have argued for a very long time that we

**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.**

1908 should be moving to this technology as quickly as possible  
1909 because of its proven fraud protection and because in the  
1910 context of today's hearing, that it has an important effect  
1911 and devaluing the data that businesses hold. So the  
1912 information that flows through a retailers system, at the  
1913 point of sale, would be rendered useless to criminals if they  
1914 were able to captured, if you use the chip and PIN system.  
1915 We think it is absolutely critical.

1916 To your point about evolving technologies, that is  
1917 absolutely true. It is the best technology. Chip and PIN is  
1918 the best technology that is available today, and we are years  
1919 behind the rest of the world in catching up to it. And as a  
1920 result, we are behind. When chip and PIN was introduced in  
1921 Europe, we saw fraud flow in two directions, online in Europe  
1922 to you point and to the United States because it became the  
1923 lowest common denominator.

1924 As for long-term solutions, we believe the chip and PIN  
1925 serves a near-term need, and we need to evolve to next  
1926 generation because as you suggest, the world is moving  
1927 online. E-commerce is booming on line.

1928 Mr. {Bilirakis.} Thank you very much. The next

**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.**

1929 question is for the entire panel. Some of the recent data  
1930 breaches were caused by third parties, such as contractors.  
1931 What recommendations would you make if any to address when  
1932 these situations occur? We will start over here, if that is  
1933 okay with Ms. Hyman.

1934 Ms. {Hyman.} Well, first of all, with regard to third  
1935 parties, again, many of our member companies are solution  
1936 providers, those third parties that you may be talking about.  
1937 Human error continues to be one of the greatest causes of  
1938 data breach, and I think doing best practices for the  
1939 industry and for all companies involved on how to mitigate  
1940 some of those human errors is very important. Education,  
1941 ongoing efforts, we have an IT trust mark, security trust  
1942 mark, which is a benchmark for an organization to undertake  
1943 appropriate practices for data security. So all of these  
1944 pieces come into play, but having a standard for data breach  
1945 notification also puts everybody on notice about what the  
1946 consumer needs to know in a timely and actionable way.

1947 Mr. {Bilirakis.} Mr. Dodge?

1948 Mr. {Dodge.} The questions about third-party--

1949 Mr. {Bilirakis.} The third party, with regard to third

**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.**

1950 parties, correct.

1951 Mr. {Dodge.} Yeah. So we think that it is important.

1952 It is important incentive that the breached entity be

1953 obligated to make the notice, but flexibility should exist

1954 for parties to contractually determine in the instance of a

1955 breach who should issue the notice.

1956 Mr. {Bilirakis.} Thank you. Yes, ma'am.

1957 Ms. {Barrett-Glasgow.} As a vendor, we see lots of

1958 increasing requirements from our clients to not only adhere

1959 to security standards but to have indemnification if a breach

1960 occurs in our environment of the data that we are holding and

1961 processing for them.

1962 Mr. {Bilirakis.} Thank you. Mr. Hartzog?

1963 Mr. {Hartzog.} My recommendation would be maybe, if

1964 there is even a possible compromise here, which is if

1965 breached entities have no relationship to the consumer whose

1966 data they hold. Then perhaps there could be some kind of

1967 requirement where you would have to disclose the relationship

1968 to the--say we got this information from an entity that

1969 collected your personal information which is why you don't

1970 recognize us. But we were breached. So that could be one

**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.**

1971 way to handle that.

1972 Mr. {Bilirakis.} Okay, Mr. Chairman. I actually have  
1973 one more question if you--

1974 Mr. {Burgess.} Ask unanimous consent that the gentleman  
1975 be able to ask his question. Without objection, so ordered.

1976 Mr. {Bilirakis.} Thank you.

1977 Mr. {Burgess.} It is an immense power that I wield  
1978 here, Gus.

1979 Mr. {Bilirakis.} Okay, for the panel again, keeping in  
1980 mind the touchstone of this process is notifying an  
1981 individual in the event that they need to mitigate the  
1982 economic risks associated with a breach, which entity is in  
1983 the best position to notify individuals after a breach? Is  
1984 there a reason to deviate from the structure that the States  
1985 have used? And we will start with Ms. Hyman, please.

1986 Ms. {Hyman.} Are you asking in terms of who is  
1987 responsible for the notification or which enforcement agency?

1988 Mr. {Bilirakis.} Who would be responsible for the  
1989 notification.

1990 Ms. {Hyman.} We want to make sure that we are, again,  
1991 not over-notification or confusing the consumer. So 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.**

1992 entity with which they have provided their information to  
1993 that would have done the transaction would be the first  
1994 source. Then contractually--and I come back to the previous  
1995 question about third parties. There are contractual  
1996 relationships beyond that.

1997 Mr. {Bilirakis.} Again, with regard to the States, how  
1998 would you--

1999 Ms. {Hyman.} We said that the State Attorneys General  
2000 should have enforcement opportunities. If it is also the FTC  
2001 that is undertaking enforcement, one should extinguish the  
2002 other. They should not happen simultaneously.

2003 Mr. {Bilirakis.} Very good. I am sorry. I am having a  
2004 little trouble hearing. I apologize. Mr. Dodge, please.

2005 Mr. {Dodge.} Sure. We strongly believe that the  
2006 obligation to notify should be with the breached entity and  
2007 then again, flexibility among parties to contractually  
2008 determine who sends the notification, if it makes more sense  
2009 for somebody else to send it. And we agree the State  
2010 Attorneys General have an important role to play in this.

2011 Mr. {Bilirakis.} Very good. Thank you. Please.

2012 Ms. {Barrett-Glasgow.} In the interest of time, I will

**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.**

2013 agree.

2014 Mr. {Bilirakis.} Okay. Very good.

2015 Mr. {Hartzog.} And I would agree that the current  
2016 trajectory of the State law is what I would recommend.

2017 Mr. {Bilirakis.} Thank you very much. I appreciate it.  
2018 I yield back, Mr. Chairman. Thanks for allowing me to ask  
2019 that last question.

2020 Mr. {Burgess.} The chair thanks the gentleman. The  
2021 gentleman does yield back. Seeing no further members wishing  
2022 to ask questions, I would like to thank the witnesses and  
2023 members for their participation in today's hearing. Before  
2024 we conclude, I would like to include the following documents  
2025 to be submitted for the record by unanimous consent: a  
2026 letter on behalf of the Consumer Electronics Association; a  
2027 letter on behalf of the Direct Marketing Association; a joint  
2028 letter on behalf of the American Bankers Association, the  
2029 Consumer Bankers Association, the Credit Union National  
2030 Association, Financial Services Roundtable, Independent  
2031 Community Bankers Association, the National Association of  
2032 Federal Credit Unions; an additional letter on behalf of the  
2033 Marketing Research Association; a letter on behalf 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.**

2034 National Retail Federation; a letter on behalf of the  
2035 National Association of Federal Credit Unions; a joint letter  
2036 on behalf of the Consumer Data Industry Association, the  
2037 Interactive Advertising Bureau, the National Business  
2038 Coalition on E-Commerce and Privacy, and the National Retail  
2039 Federation, the United States Chamber of Commerce; and a  
2040 joint statement for the record on behalf of the National  
2041 Association of Convenience Stores and the Society of  
2042 Independent Gasoline Marketers of America.

2043 Pursuant to committee rules, I remind members that they  
2044 have 10 business days to submit additional questions for the  
2045 record, and I ask the witnesses submit their response within  
2046 10 business days upon receipt of the questions.

2047 Without objection, all of the statements are entered  
2048 into the record.

2049 [The information follows:]

2050 \*\*\*\*\* 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.**

|

2051           Mr. {Burgess.} And without objection the subcommittee

2052 is adjourned.

2053           [Whereupon, at 12:47 p.m., the Subcommittee was

2054 adjourned.]