

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed 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 HIF199.170

4 ``REPORTING DATA BREACHES: IS FEDERAL LEGISLATION NEEDED TO

5 PROTECT CONSUMERS?''

6 THURSDAY, JULY 18, 2013

7 House of Representatives,

8 Subcommittee on Commerce, Manufacturing, and Trade

9 Committee on Energy and Commerce

10 Washington, D.C.

11 The Subcommittee met, pursuant to call, at 11:04 a.m.,  
12 in Room 2123 of the Rayburn House Office Building, Hon. Lee  
13 Terry [Chairman of the Subcommittee] presiding.

14 Present: Representatives Terry, Lance, Harper, Guthrie,  
15 Olson, Kinzinger, Bilirakis, Johnson, Long, Barton,  
16 Schakowsky, Sarbanes, McNerney, Barrow, Christensen 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.**

17 Waxman (ex officio).

18 Staff present: Kirby Howard, Legislative Clerk; Nick  
19 Magallanes, Policy Coordinator, Commerce, Manufacturing, and  
20 Trade; Brian McCullough, Senior Professional Staff Member,  
21 Commerce, Manufacturing, and Trade; Gib Mullan, Chief  
22 Counsel, Commerce, Manufacturing, and Trade; Andrew Powaleny,  
23 Deputy Press Secretary; Shannon Weinberg Taylor, Counsel,  
24 Commerce, Manufacturing, and Trade; Michelle Ash, Democratic  
25 Chief Counsel; and Will Wallace, Democratic Professional  
26 Staff Member.

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

|  
27           Mr. {Terry.} Good morning. I recognize myself for an  
28 opening statement.

29           In today's economy, nearly everyone leaves a digital  
30 footprint. Even if you made a concerted effort to avoid  
31 smartphones, laptops and social media, although I have not  
32 found that person, you would have a difficult time keeping  
33 your personal information from being held in an electronic  
34 database somewhere.

35           Consumers should have the peace of mind that their data  
36 is protected in a responsible way. But with all types of  
37 nefarious activities online, cyber criminals are finding new  
38 ways and, frankly, seem to be very consistent in their wishes  
39 to steal data. So in the event that our personal data  
40 becomes exposed, we need to be able to trust that the  
41 companies in possession of that data will notify us of the  
42 exposure. And certainly it is in those companies' best  
43 interest to notify promptly and clearly in order to preserve  
44 a trusting relationship with their customers.

45           Given these considerations, the question before us is:  
46 What are the rules of the road for companies that experience

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

47 a breach in their data stores? Currently, the laws that  
48 govern data breach notification are a patchwork of State- and  
49 territory-specific statutes. Unfortunately, they tend to  
50 differ from each other in many ways. For example, while a  
51 number of States have adopted a common definition of personal  
52 information, even more States have adopted alterations to  
53 that definition, and those vary unpredictably. The  
54 definition is important because it triggers the duty to  
55 notify of a breach. Three States include encrypted or  
56 redacted data in the definition of personal information,  
57 whereas the rest do not. Five States include public records  
58 in the definition. Meanwhile, four States protect an  
59 individual's date of birth and mother's maiden name as  
60 personal information.

61 With at least 48 of these various State- and territory-  
62 specific laws on the books, you can see how the cost of  
63 compliance could add up. The global price tag of cyber crime  
64 has been calculated at around \$110 billion annually, and we  
65 should not add unnecessary compliance costs to this. Adding  
66 to the confusion, these laws also tend to vary on the number  
67 of days that can elapse after a breach before notification as

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

68 well as the method of notification.

69 Even small breaches can cause a compliance headache. In  
70 one recent example, a large company experienced a breach  
71 where the personal information of just over 500 consumers was  
72 compromised. In comparison to other breaches involving tens  
73 of millions of consumers, this may seem small. Yet it turns  
74 out that these 500 consumers lived in 44 different States and  
75 therefore had to be notified pursuant to 44 different sets of  
76 rules.

77 We must remember that where a breach in data is an  
78 intentional intrusion from the outside, for example, if it is  
79 done by a hacktivist, a foreign agent or a run-of-the-mill  
80 criminal, the company holding the data is also a victim.  
81 Burdening these entities with overly complicated notification  
82 rules is not a solution to the harms that result from the  
83 exposure of that personal information held by the company.

84 And with that, I look forward to hearing the testimony  
85 of our witnesses and learning about whether or not we can  
86 improve the current legal landscape for breach notification.

87 [The prepared statement of Mr. Terry follows:]

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

88 \*\*\*\*\* 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.**

|  
89 Mr. {Terry.} At this point, I will yield back my time  
90 and recognize the ranking member, Jan Schakowsky, for her  
91 statement.

92 Ms. {Schakowsky.} Thank you, Mr. Chairman.

93 Apropos of this hearing, it has just been reported this  
94 very morning that Anonymous claims to have hacked into 1,800  
95 email accounts of Members of Congress and their staffs. So  
96 that is apparently in the news. I don't know to what extent  
97 that has been confirmed. So I look forward to hearing from  
98 our witnesses about this issue and steps that can and should  
99 be taken to address it.

100 As a long-time consumer advocate, I believe that the  
101 public does have a right to be informed if their personal  
102 information such as names, email addresses, passwords, home  
103 addresses, health and financial data is compromised. As more  
104 and more information moves online, it is equally important to  
105 ensure that precautions are taken to keep that data secure.

106 Less than 2 years ago following the breaches of data at  
107 Citicorp, Epsilon and Sony, a report of the data security  
108 from Protegrity found that personal information was ``highly

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

109 valuable'' to cyber criminals but ``vastly unprotected.``  
110 Since then, it seems to me, and you will set me straight,  
111 little has changed. Last year, 680 confirmed data breaches  
112 compromised almost 28 million records. Many of those could  
113 have been prevented with relative ease had the entities  
114 holding the data followed known best practices. This is  
115 clearly a major issue which the private sector has not done  
116 enough on its own to address, and one of great concern, I  
117 believe, to the public.

118       Almost every State and territory including my home State  
119 of Illinois has adopted data breach standards. While  
120 national standards might be needed to adequately address this  
121 issue, I want to make clear, my view is that any federal law  
122 should not weaken strong State laws. In addition, any  
123 federal response should establish a baseline so that every  
124 American can be assured some level of data protection, not  
125 just notification after the fact.

126       This subcommittee has several questions to answer as we  
127 consider data breaches and hopefully data security as well.  
128 What specific measures should be taken to protect personal  
129 information stored online? When should consumers be notified

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

130 of a breach? What role should the federal government play in  
131 ensuring that those steps are taken? I believe that entities  
132 that store important data should act proactively to defend  
133 that information and the consumer should be notified if a  
134 breach could result in personal harm.

135 The DATA Act, introduced by Mr. Rush and passed by voice  
136 vote just 4 years ago, would have taken those steps to  
137 protect American consumers. I was a cosponsor of that bill  
138 along with Mr. Barton, and I believe it should be the  
139 framework for bipartisan legislation in this Congress.

140 Again, I look forward to hearing from our witnesses  
141 today about what can and should be done to address breach  
142 notification and data security. I hope that this  
143 subcommittee can work constructively toward a bipartisan  
144 solution to this major issue that impacts all of us.

145 Thank you. I yield back.

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

147 \*\*\*\*\* 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.**

148 Mr. {Terry.} And that is our goal.

149 At this time the chair recognizes the chairman emeritus,  
150 Mr. Barton.

151 Mr. {Barton.} Thank you, Mr. Chairman, and I am very  
152 happy that you are having this hearing. As Congresswoman  
153 Schakowsky just pointed out, this is an issue that is not  
154 unfamiliar to the subcommittee or the full committee. Going  
155 back to my tenure as chairman in 2005 and 2006, we passed a  
156 bill out of committee but it didn't go to the Floor. Under  
157 Mr. Dingell's chairmanship and Mr. Waxman's chairmanship,  
158 again, we passed bills that came out of committee and we have  
159 even had one bill that passed the Floor of the House but it  
160 wasn't taken up in the Senate. The last Congress, we passed  
161 a bill out of this subcommittee but it was not taken up at  
162 full committee.

163 So this is an issue that we all have general agreement  
164 on. As Congresswoman Schakowsky has pointed out, it is not a  
165 partisan issue. Hopefully under your leadership, Mr.  
166 Chairman, and Mr. Upton's leadership at the full committee,  
167 we will pass something in this committee, on the Floor 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.**

168 get the other body to take it up.

169           This year alone, our last year, in 2012, there were 470  
170 breaches that meet the definition, and so far this year,  
171 there have been 326 breaches. This is an issue that is not  
172 going to go away. It would appear to be obvious that we need  
173 a federal bill instead of a patchwork of State bills, and I  
174 would agree with what Congresswoman Schakowsky said, that a  
175 federal bill should be a baseline bill and not a bill that  
176 limits the States.

177           With that, Mr. Chairman, again, thank you for your  
178 leadership. I believe you are the man who can make this  
179 happen, subcommittee, full committee, the Floor and then with  
180 the other body. And with that, I will yield back.

181           [The prepared statement of Mr. Barton follows:]

182           \*\*\*\*\* 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.**

183           Mr. {Terry.} No pressure there.

184           Are there any other Republicans on this side that wish  
185 to have time yielded?

186           Mr. {Barton.} If not, Mr. Chairman, I yield back.

187           Mr. {Terry.} Then we will yield back.

188           Before I announce our panel and start our testimony, an  
189 announcement of sorts--oh, Henry is here, so while he is  
190 sitting down, my announcement is, we will recess at noon and  
191 reconvene if it is still necessary to. I have a feeling that  
192 there is going to be enough questions that we will reconvene  
193 at 1 o'clock but break at noon, and I recognize the full  
194 committee ranking member, the gentleman from California is  
195 recognized for 5 minutes.

196           Mr. {Waxman.} Thank you very much, Mr. Chairman. I  
197 welcome all of our witnesses today.

198           Our subcommittee is going to address the federal role in  
199 data breach notification. It is alarming just how common  
200 data breaches have become. Since 2005, at least 600 million  
201 records containing consumers' personal information have been  
202 compromised as a result of more than 3,800 data breaches 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.**

203 the United States. At least 72 million personal records have  
204 been compromised only in the time since July 2011, when the  
205 Subcommittee last considered this issue.

206 Every type of entity has proven vulnerable, including  
207 private sector companies of all sizes, colleges and  
208 universities, and federal, State, and local governments.  
209 Breaches result from a wide variety of causes. External  
210 criminal attacks, dishonest insiders, and simple negligence  
211 can all be responsible for compromising consumers' personal  
212 information. Moreover, in recent months, it has become  
213 abundantly clear that commercial data breaches can also  
214 result from State-affiliated cyber attacks.

215 Consumers face severe threats to their financial well-  
216 being when data like banking information or Social Security  
217 numbers are compromised. In 2012 alone, more than 12 million  
218 U.S. adults were victims of identity theft or similarly  
219 costly forms of fraud. Less reported, but also of concern,  
220 is when breaches, non-financial in nature, threaten  
221 consumers' privacy, including breaches involving health-  
222 related information, biometric data, or a person's precise  
223 location.

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

224           Nearly all U.S. States and territories now have laws  
225 that require notice for their own residents when a data  
226 breach occurs. These laws vary greatly, but several of these  
227 laws are quite strong, ensuring that consumers receive  
228 prompt, clear and complete notification when their personal  
229 information is breached and providing them with resources to  
230 protect their financial well-being. I am glad that these  
231 laws have been enacted, but after-the-fact breach  
232 notification is only half of what is needed. The private  
233 sector also must take reasonable steps to safeguard personal  
234 information.

235           When it comes to information security, prevention is the  
236 best medicine. Research shows that the vast majority of  
237 attacks on commercial data--78 percent according to the  
238 Verizon RISK Team--utilize simple tactics easily thwarted by  
239 basic security infrastructure and procedures.

240           There are many companies that take information security  
241 very seriously and work diligently to combat this problem,  
242 and perhaps there will always be cyber crime. But  
243 unfortunately, there are also companies that are not doing  
244 enough to prevent breaches, and consumers are paying 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.**

245 price.

246 As the subcommittee moves forward with its work on  
247 information security, I strongly encourage all members to  
248 keep two points in mind. First, federal legislation must not  
249 move backward by undermining those States with strong breach  
250 notification laws. And second, effective security for  
251 consumers' personal information indisputably requires both  
252 breach notification and reasonable safeguards for commercial  
253 data.

254 I look forward to the testimony we are going to get  
255 today and our discussion of this issues today and in the  
256 future and I hope we can work together to deal with this  
257 important issue.

258 [The prepared statement of Mr. Waxman follows:]

259 \*\*\*\*\* 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.**

260 Mr. {Terry.} I appreciate that, Mr. Chairman.

261 At this time I am going to introduce our full panel, and  
262 then we will start with Mr. Richards. Mr. Richards is the  
263 Senior Vice President of Federal Government Affairs for  
264 TechAmerica. We have Dan Liutikas, Chief Legal Officer,  
265 CompTIA. We have Mr. Jeff Greene, Senior Policy Counsel,  
266 Cybersecurity and Identity, Symantec Corporation. We then  
267 have Debbie Matties, CTIA-The Wireless Association Vice  
268 President of Privacy. We have Andrea Matwyshyn, Assistant  
269 Professor of Legal Studies and Business Ethics at the Wharton  
270 School, University of Pennsylvania. David Thaw will complete  
271 our testimony, and he is Visiting Assistant Professor of Law  
272 at the University of Connecticut School of Law.

273 You will see little lights down there. Green means go.  
274 At 4 minutes, the yellow line will come on and that should be  
275 a sign, if you got a full page or two left, you may want to  
276 skip to the conclusion. The red light means I'm going to  
277 lightly tap the gavel, and so I appreciate keeping it to the  
278 5-minute mark, especially since we have been kind of put on  
279 an awkward, tight schedule today.

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

280           So Mr. Richards, you may begin. You are recognized for  
281 your 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.**

|  
282 ^STATEMENTS OF KEVIN RICHARDS, SENIOR VICE PRESIDENT, FEDERAL  
283 GOVERNMENT AFFAIRS, TECHAMERICA; DAN LIUTIKAS, CHIEF LEGAL  
284 OFFICER, COMPTIA; JEFFREY GREENE, SENIOR POLICY COUNSEL,  
285 CYBERSECURITY AND IDENTITY, SYMANTEC CORPORATION; DEBBIE  
286 MATTIES, VICE PRESIDENT OF PRIVACY, CTIA-THE WIRELESS  
287 ASSOCIATION; ANDREA M. MATWYSHYN, ASSISTANT PROFESSOR OF  
288 LEGAL STUDIES AND BUSINESS ETHICS, THE WHARTON SCHOOL,  
289 UNIVERSITY OF PENNSYLVANIA; AND DAVID THAW, VISITING  
290 ASSISTANT PROFESSOR OF LAW, UNIVERSITY OF CONNECTICUT SCHOOL  
291 OF LAW

|  
292 ^STATEMENT OF KEVIN RICHARDS  
  
293 } Mr. {Richards.} Thank you. Mr. Chairman, Ranking  
294 Member Schakowsky and distinguished members of the  
295 subcommittee, thank you for the opportunity to testify today  
296 and for convening this hearing on the important issue of data  
297 breach notification. I am Kevin Richards, Senior Vice  
298 President of Federal Government Affairs of TechAmerica, a  
299 leading technology association representing the world's

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

300 premiere technology companies from the information and  
301 technology communications sector at the State, federal and  
302 international level.

303         The topic of today's hearing is an issue of great  
304 concern to our members who view the unauthorized disclosure  
305 and use of personal information as a threat that erodes  
306 public confidence in a connected world. TechAmerica's member  
307 companies understand better than anyone the nature of cyber  
308 threats that America faces today and what must be done in  
309 order to protect consumers' information from data breaches.

310         The rapid growth of the collection of information in  
311 electronic form has provided consumers, businesses and  
312 governments with tremendous opportunities from  
313 revolutionizing the way medical care is provided to enhancing  
314 government services, to enabling a free Internet with more  
315 opportunities appearing daily. However, this collection of  
316 data has also resulted in a concomitant exposure of companies  
317 to risks and liabilities arising from the collection, use,  
318 storage and transmission of information, particularly  
319 sensitive information about individuals.

320         TechAmerica strongly believes that if a breach occurs

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed 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 that poses a significant risk of serious harm, that there  
322 should be a consistent national policy to ensure that  
323 customers and consumers are notified in an appropriate  
324 manner.

325       Today, 48 different State jurisdictions in the United  
326 States have data breach notification laws, and while many  
327 businesses have managed to adapt to these various laws, a  
328 properly defined data breach notification standard would go a  
329 long way to guide organizations on how to address cyber  
330 threats in their risk management policies. It also would  
331 help prevent breaches and give guidance on how best to  
332 respond if an organization should fall victim to a reach  
333 caused by an attack. It would be particularly helpful for  
334 smaller businesses, many of whom cannot afford teams of  
335 lawyers to navigate 48 breach standards should something bad  
336 actually happen.

337       National data breach legislation should be carefully  
338 crafted and in particular be technology-neutral to help  
339 organizations prevent and respond to security incidents while  
340 avoiding costly, burdensome rules that would not provide any  
341 real protection to consumers and free security innovation.

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed 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 Such legislation will provide much-needed regulatory relief  
343 to companies facing conflicting legal obligations under  
344 today's patchwork of State laws.

345 TechAmerica has been a leader in calling for a strong,  
346 preemptive and uniform national breach notification law.  
347 Federal legislation that promotes notification to consumers  
348 when their data has been compromised is needed, and can  
349 effectively help restore consumers' online trust and  
350 confidence.

351 The first objective of federal data breach notification  
352 legislation should be to establish a uniform national  
353 standard and preempts the current patchwork of existing State  
354 laws while providing a safe harbor for those entities that  
355 take steps to protect their systems from breaches and render  
356 data unreadable, undecipherable and unusable in order to  
357 protect individuals from harm. The following recommendations  
358 are a result of lessons learned from the implementation of  
359 regimes by the current 48 different State jurisdictions in  
360 the United States and which serve as a good benchmark for  
361 drafting potential legislation.

362 One, legislation must establish a single, uniform

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

363 preemptive standard. Two, a meaningful threshold for  
364 notification should be established. Three, define carefully  
365 the kind of personally identifiable information that is  
366 covered by notification requirements. Four, avoid mandating  
367 specific technologies while encouraging the adoption of good  
368 practices. Five, when third-party managed data notification  
369 is required, avoid consumer confusion. Six, a federal law  
370 should do more than the patchwork of State laws to protect  
371 consumers.

372 In conclusion, TechAmerica believes that the patchwork  
373 quilt of state laws and existing requirements needs to be  
374 overhauled by a uniform preemptive national standard based on  
375 the risk of harm. This would be in addition to the  
376 significant protection consumers receive today. With the  
377 chairman's permission, TechAmerica would like to request the  
378 submission of TechAmerica's national data breach legislative  
379 principles for inclusion in the record for today's hearing.

380 Mr. {Terry.} Unanimous consent to allow? Hearing no  
381 objection, so allowed.

382 Mr. {Richards.} Thank you. We are happy to offer  
383 assistance to the committee and work with you as 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.**

384 legislative process moves forward.

385 Thank you for allowing me the privilege to appear today  
386 in order to share TechAmerica's views on the important of  
387 data breach notification. I would be happy to answer any  
388 questions that the committee may have at this time.

389 [The prepared statement of Mr. Richards follows:]

390 \*\*\*\*\* 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.**

|  
391 Mr. {Terry.} Thank you very much.

392 And now, Mr. Liutikas, you have your 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.**

|  
393 ^STATEMENT OF DAN LIUTIKAS

394 } Mr. {Liutikas.} Good morning, Chairman Terry, Ranking  
395 Member Schakowsky and distinguished members of the House  
396 Subcommittee on Commerce, Manufacturing, and Trade. This  
397 testimony is submitted on behalf of the 2,000 members of the  
398 Computing Technology Industry Association, also known as  
399 CompTIA, a not-for-profit trade association.

400 CompTIA is also the leading developer and provider of  
401 vendor-neutral education, IT workforce certifications  
402 including A+, Security+ and Network+, and organizational  
403 credentials such as the Security Trust Mark.

404 My name is Dan Liutikas, and I am the Chief Legal  
405 Officer of CompTIA. Prior to CompTIA, I was an attorney in  
406 private practice focusing on corporate technology and  
407 intellectual property matters, primarily for the small- to  
408 medium-size business. I am a native of Chicago, Illinois,  
409 and was born to immigrant parents from Lithuania. My father  
410 opened his own television repair shop and then later started  
411 a construction business. My mother started her own

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

412 restaurants, delis and banquet halls. Both lived the  
413 American dream by being entrepreneurial and starting their  
414 own small businesses. From my own experience, I submit that  
415 small business owners don't want handouts.

416 Like the businesses started by my parents, many of our  
417 members are small- to medium-sized businesses expect that  
418 they are IT solution providers that help other small- to  
419 medium-sized businesses set up IT systems and manage data.  
420 They also just want a fair shot at pursuing the American  
421 dream. In the context of today's hearing, that means  
422 eliminating unnecessary barriers to entry such as redundant  
423 and burdensome regulations. With that context, let me state  
424 upfront that our membership supports a federal approach to  
425 data breach notification.

426 It is hard to believe that it has been 10 years since  
427 California became the first State in the country to enact a  
428 State data breach notification law. Today, there are 46  
429 States, D.C. and several territories that enacted data breach  
430 notification laws. Data breach notification standards are  
431 clearly a relevant concern for millions of users sharing  
432 information through the Internet and for information being

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

433 stored in various forms.

434 A federal approach will bring clarity and certainty not  
435 only to small businesses but also to consumers who may not be  
436 aware of the notice obligations of a particular State's data  
437 breach notification law or even when such obligations may  
438 apply.

439 We appreciate the opportunity to submit our written  
440 testimony that provides greater details on the burdens of the  
441 current patchwork of State laws and the way in which  
442 advancements in mobile technology exacerbate those burdens.  
443 Therefore, i would like to spend the balance of my time on a  
444 solution.

445 Based on our collective experience and outreach efforts,  
446 we believe that the IT industry will be receptive to a  
447 national data breach reform framework that contains the  
448 following six principles.

449 Number one, there should be a single national federal  
450 standard for data breach policy. Businesses which conduct  
451 commerce over multiple States need the certainty and  
452 efficiency that a national standard would provide.

453 Number two, Congress and the FTC should not mandate

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

454 specific technology or methods for data security practices.  
455 The environment for data security is constantly evolving, so  
456 any regulation should focus on promoting validated industry  
457 standards for security, rather than a single quickly outdated  
458 solution.

459         Number three: There should be an exemption from  
460 notification requirement for entities that deploy technology  
461 or methods such as encryption and other technologies that  
462 render data unusable or unreadable by hackers as a harm-  
463 prevention measure.

464         Number four, all enforcement and penalties for data  
465 breach law should be administrated by a central government  
466 agent instead of State Attorneys General, except in cases  
467 where the federal agent can or has not acted.

468         Number five, entities compliant with existing data  
469 breach legislation such as the Gramm-Leach-Bliley Act should  
470 be exempt from new regulation. We should not reinvent the  
471 wheel or create conflicting or overlapping regulations.

472         And number six, notification should occur on a  
473 reasonable time frame, which includes allowances for risk  
474 assessment and any necessary law enforcement procedures or

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

475 investigation. Notification should be focused on events  
476 where there is a possibility of actual harm including a  
477 minimum threshold of affected individuals.

478 In closing, I want to reiterate that we believe that a  
479 national data breach framework is in the best interest of  
480 both consumers and small- to medium-sized businesses.

481 Thank you again for the opportunity to share our  
482 perspective on the issue of data breach notification reform,  
483 and I look forward to our discussion on how to best approach  
484 this issue, and I would be happy to answer any questions.

485 [The prepared statement of Mr. Liutikas follows:]

486 \*\*\*\*\* 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.**

|  
487 Mr. {Terry.} Thank you very much.

488 Mr. Greene, you are now 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.**

|  
489 ^STATEMENT OF JEFFREY GREENE

490 } Mr. {Greene.} Chairman Terry, Ranking Member  
491 Schakowsky, members of the subcommittee, thank you for the  
492 opportunity to testify today on behalf of Symantec  
493 Corporation. We are the largest security software company in  
494 the world with 31 years of experience in developing Internet  
495 security technology.

496 For organizations that have critical information assets,  
497 the risk of a data breach has really never been higher than  
498 it is now. We estimate that last year, there were 93 million  
499 identities exposed. Thankfully, few of these victims will  
500 have his or her identity stolen or bank account raided, but  
501 the reality is that all of them are at risk for it because  
502 once your information has been stolen, you can do little more  
503 than hope that no one tries to monetize it.

504 The costs of these breaches is real. Mr. Chairman, as  
505 you mentioned in 2012, our Norton cyber crime report put the  
506 global price tag of consumer cyber crime at \$110 billion, and  
507 that is just the consumer side. On the business side, 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.**

508 Ponemon Institute estimated that in 2012, the average  
509 organizational cost for a breach in the United States was  
510 \$5.4 million.

511 Breaches can be caused most commonly or very commonly by  
512 lost computers or portable media, and they can be caused by  
513 outright theft--people that walk out the door with sensitive  
514 information, disgruntled or fired employees. But there is  
515 another cause for breaches, and that is targeted attacks, and  
516 actually last year, according to our Internet Security Threat  
517 report, 40 percent of breaches were caused by targeted  
518 attacks and hackers. Most of these attacks rely on social  
519 engineering, basically trying to trick people into doing  
520 something on their computer that they were never do if they  
521 were fully cognizant of their actions. We also saw a lot of  
522 email attacks. It is still a very common vector. And we  
523 regularly see criminals mining social media to come up with  
524 tidbits about individuals they use to craft emails that will  
525 look legitimate, even to very cautious users. Twenty twelve  
526 also saw the emergence of what we call watering hole attacks.  
527 Like the proverbial lion in the jungle who waits by the  
528 watering hole for unsuspecting prey, cyber criminals 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.**

529 become adept at compromising legitimate Web sites and then  
530 sitting on them and waiting for visitors to come by and then  
531 attempting to compromise every one who visits.

532         The growing use of the cloud also presents unique  
533 challenges and opportunities. Cloud done right is an  
534 opportunity for very strong security. You are putting your  
535 data behind higher walls and having it watched by more walls.  
536 Cloud done wrong, though, can be a recipe for data breach  
537 because you are grouping your data with many other people's,  
538 creating a very desirable target for attackers and one that  
539 is not well defended.

540         As you mentioned, Mr. Chairman, mobile devices require  
541 strong security. We are all doing more and more of our lives  
542 on mobile computers, and unfortunately, the criminals are  
543 following. Last year, we saw a 58 percent increase in the  
544 types of malware that were designed specifically for mobile  
545 devices, and even since we released our report in April, we  
546 have seen dramatic evidence of the increasing focus on mobile  
547 attacks.

548         Good security really starts with the basics--patch  
549 management, updating your patches on your computer, 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.**

550 strong passwords. The breach that the ranking member  
551 indicated was reported this morning, based on the early  
552 reporting, there was a significant number of people who were  
553 using the word ``password'' as their password. That is just  
554 not a strong password; you are asking for it.

555         So-called zero days or previously unknown critical  
556 vulnerabilities receive a lot of media attention, but  
557 unfortunately, it is still well-known older vulnerabilities  
558 that cause most patches. Modern security software is  
559 essential. I am not talking about the proverbial your  
560 father's antivirus anymore. Modern security software will  
561 monitor your computer looking for anomalous Internet  
562 activity, processes or other system events that could be  
563 indicative of a previously known infection. We have  
564 reputation-based technology we use that actually looks at  
565 individual files based upon their frequency we see out in the  
566 wild and we are able to detect previously unknown threats  
567 just by looking at a file that way.

568         Looking at the legal landscape, we do support a national  
569 standard for breach notification, and we have identified  
570 three principles that are key to us. First, the scope of any

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

571 legislation should include all entities that collect,  
572 maintain or sell significant numbers of records containing  
573 sensitive personal information, and we think that that should  
574 apply equally to the government and to the private sector.  
575 Second, pre-breach security measures should be central to any  
576 legislation. New legislation should seek to minimize the  
577 likelihood of a breach and not just focus on what to do  
578 afterward. And finally, any notification scheme should  
579 minimize false positives. Promoting technology like  
580 encryption as a best practice would significantly reduce  
581 these false positives and limit the burden on consumers and  
582 on businesses.

583 I thank you again for the opportunity and the privilege  
584 to testify today. I look forward to your questions.

585 [The prepared statement of Mr. Greene follows:]

586 \*\*\*\*\* 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.**

|  
587 Mr. {Terry.} Thank you very much.

588 Ms. Matties, you are 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.**

|  
589 ^STATEMENT OF DEBBIE MATTIES

590 } Ms. {Matties.} Chairman Terry, Ranking Member  
591 Schakowsky and the members of the subcommittee, thank you for  
592 the opportunity to participate in today's hearing. My name  
593 is Debbie Matties, and I am the Vice President for Privacy at  
594 CTIA.

595 CTIA along with AT&T, Comcast, DIRECTV, NCTA, Time  
596 Warner Cable, USTelecom and Verizon is a member of the 21st  
597 Century Privacy Coalition. The Coalition seeks to modernize  
598 U.S. privacy and data security laws to better serve consumers  
599 as well as to reflect the ways that communications technology  
600 and competition has changed in the last two decades.

601 CTIA commends the subcommittee for exploring whether  
602 federal data breach legislation is necessary to protect  
603 consumers. Today's patchwork of State and federal data  
604 security and breach notification laws is complicated for  
605 businesses and provides uneven protection for consumers. A  
606 strong, comprehensive and streamlined federal framework  
607 enforced by a single agency would create more certainty for

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

608 businesses and better protect consumers from the harms  
609 associated with data breaches.

610 Today's variety of State and federal requirements  
611 creates inconsistent, sometimes contradictory responses to  
612 breaches that do not benefit consumers. For example, some  
613 States require breach notifications to occur ``without  
614 unreasonable delay'' whereas other States require specific  
615 time frames for notification. Some states provide an  
616 exemption for notification for immaterial breaches whereas  
617 other States do not.

618 Most data breaches impact consumers in multiple States,  
619 just like the breach that happened here in the House, and  
620 electronic data is rarely segmented by State. So under law,  
621 the question becomes, which State law should apply? The  
622 State in which the consumer resides? The State in which the  
623 breach occurred or the State in which a vulnerability existed  
624 and was exploited? For wireless consumers using family  
625 plans, often the user of a device is in a different State  
626 from the subscriber who pays the bill. Given the fact that  
627 breaches inevitably transcend State borders, a federal  
628 approach to breach notification is appropriate so that 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.**

629 consumers receive the same benefits.

630           The absence of a consistent nationwide regime also  
631 creates unnecessary distraction for companies that need to  
632 stop a breach, evaluate the damage caused by the breach and  
633 its scope, correct whatever vulnerability resulted in the  
634 breach, work with law enforcement to investigate the breach,  
635 and of course, most important, notify consumers to help  
636 mitigate any harm. These time-sensitive activities are  
637 hampered when a company, especially a small business, has to  
638 evaluate which of the 48 different State regimes applies to  
639 each of their customers and then tailor breach notifications  
640 accordingly. It also makes it difficult for consumer  
641 protection agencies, consumer advocates and businesses to  
642 educate consumers faced with a data breach about their  
643 rights.

644           Multiple federal regimes undermine consumer protection  
645 in a similar manner. For example, wireless carriers fall  
646 within the FCC'S CPNI rules to the extent they are providing  
647 a telecommunications service such as voice. But some  
648 providers of voice like Skype are not subject to CPNI rules,  
649 and then the FTC asserts data security 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.**

650 wireless carriers when they are providing Internet access.

651 In any case, the CPNI rules don't really make a lot of  
652 sense. They don't cover critically important information  
653 like name, Social Security number or credit card number but  
654 they do cover, for example, the number of voice lines a  
655 subscriber has on her plan. A unified, streamlined federal  
656 data security and breach notification law that applies  
657 equally to all entities and to all data would make consumers  
658 more confident in the security of their online information  
659 and would in turn give them greater trust in Internet  
660 commerce. This unified federal approach to data security is  
661 bipartisan and is in line with the Obama Administration's  
662 recommendations to level the playing field for companies and  
663 provide a consistent set of expectations for consumers by  
664 simplifying and clarifying the privacy laws. CTIA supports  
665 the Administration's recommendation to narrow the common  
666 carrier exemption to the extent needed to enable the FTC to  
667 enforce data security and data breach notification  
668 requirements.

669 Mr. Chairman, CTIA fully supports a unified, streamlined  
670 federal data security and breach notification law 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.**

671 enforced by the FTC and benefits consumers who expect that  
672 their information will be afforded the same high degree of  
673 protection regardless of what entity collects the  
674 information, where the consumer lives, where a breach occurs,  
675 or where hackers may be trying to access personal  
676 information. Congress should enact a new law to better  
677 reflect consumer expectations.

678 I would be happy to answer your questions.

679 [The prepared statement of Ms. Matties follows:]

680 \*\*\*\*\* 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.**

|  
681 Mr. {Terry.} Well done.

682 Professor Matwyshyn, you are now recognized for 5  
683 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.**

|  
684 ^STATEMENT OF ANDREA MATWYSHYN

685 } Ms. {Matwyszyn.} Thank you. Chairman Terry, Ranking  
686 Member Schakowsky, it is my great honor to be with all of you  
687 today to discuss a topic that I have devoted my scholarship  
688 to, and that is the question of how to improve information  
689 security in the United States.

690 I started working in this space approximately 14 years  
691 ago as a corporate attorney representing multinational  
692 clients as well as entrepreneurs in Chicago. I really  
693 watched the evolution of this space as both a member of the  
694 business community at first representing clients and now as  
695 an academic, and although there has been tremendous  
696 improvement in this space, we still have a reasonable way to  
697 go.

698 The public awareness around questions of information  
699 security has tremendously increased during the last 10 years,  
700 and it is with great pleasure that I see that we are  
701 discussing these topics today. However, the questions of  
702 conduct and reasonableness in behavior and information

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

703 security still remain unanswered.

704           With that, I would like to offer a historical example to  
705 offer perhaps a paradigm to conceptualize questions of  
706 information security. In addition to teaching Internet law  
707 and data security and privacy law, I also teach securities  
708 regulation, and I would submit that perhaps the questions  
709 that we are facing today have a historical parallel in the  
710 questions that this Congress faced when thinking about  
711 balancing the interests of consumer protection, capital  
712 formation and market stability in the 1933 and 1934 Acts.

713           Today in this context, perhaps those three elements are  
714 consumer protection, economic stability broadly in terms of  
715 securing information and preserving sectors of our economy  
716 that rely on information flows, and facilitating responsible  
717 innovation. So with those three elements, we can take a look  
718 at the broader set of questions in information security, and  
719 I would submit that perhaps we should draw a clear  
720 distinction between disclosure regulation and conduct  
721 regulation.

722           Disclosure regulation, specifically data breach  
723 notification statutes, have developed to a high degree 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.**

724 State level. We have had States function as the laboratories  
725 of experimentation, and the State statutes have shown us the  
726 way as to what is a feasible and successful approach for  
727 disclosure, and offered us guidance to at this point be able  
728 to come up with a set of criteria that can be operationalized  
729 on a national level through the Federal Trade Commission to  
730 provide us the data to be able to analyze what is going on in  
731 our economy, who are the companies that are behaving with  
732 best practices, and who are the companies that are not yet  
733 quite up to par and need to be encouraged regulatorily or  
734 otherwise on the State or national level to improve the  
735 quality of information security that they implement  
736 throughout the their organizations. The written statement  
737 that I have submitted offers a framework of this nature.

738 Conduct regulation, I would submit, we are not ready to  
739 really focus in on with a national framework yet. We need  
740 the States to show us the way, the same way that they did in  
741 the context of data breach notification. Let the States  
742 experiment, guide us, discover what works, what doesn't work,  
743 and then perhaps we can revisit this question. I would  
744 respectfully urge this body to allow for this State

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

745 experimentation and to preserve the right of States to  
746 determine recourse appropriate for their consumer harms.

747 While disclosure legislation deals with purely providing  
748 information to empower consumers to make good choices,  
749 conduct regulation is the place where we contemplate harms.  
750 This distinction, I think, would be fruitful to  
751 operationalize into a national framework for a data breach  
752 notification harmonization.

753 And in my last minute, I will highlight some of the  
754 elements that I elaborate on in detail in my written  
755 statement that may provide guidance for a federal harmonized  
756 framework.

757 First, the concept of information from a consumer and  
758 from a corporate perspective does not map onto the notion of  
759 PII that we have been working with. Sometimes the most  
760 innocuous bits of information can be the most important. If  
761 I use my favorite flavor of ice cream as my security question  
762 for my bank account, that is perhaps my most sensitive  
763 information, and so I would suggest that perhaps we should  
764 reconceptualize our notion of what constitutes consumer  
765 information in line with the way that sophisticated companies

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

766 treat information and that is around information that is  
767 shared by a consumer in a trusted relationship.

768 And with that, I will conclude because I am running out  
769 of time but I would request that this committee turn to my  
770 statement and examine the framework that I have proposed.

771 Thank you.

772 [The prepared statement of Ms. Matwyszyn follows:]

773 \*\*\*\*\* INSERT 5 \*\*\*\*\*

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

|  
774           Mr. {Terry.} We will. I appreciate you submitting

775 that.

776           Professor Thaw, you are 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.**

|

777 ^STATEMENT OF DAVID THAW

778 } Mr. {Thaw.} Thank you, Mr. Chairman.

779 Chairman Terry, Ranking Member Schakowsky, distinguished

780 members of the subcommittee, I am David Thaw, Visiting

781 Assistant Professor of Law at the University of Connecticut

782 and Fellow of the Information Society Project at Yale Law

783 School. I appreciate the opportunity to testify regarding

784 the important issues of data security and consumer

785 protection, a subject that I have spent the better part of a

786 decade researching and working on professionally.

787 Federal data breach notification is important but it

788 must be implemented properly. In my oral testimony today, I

789 wish to address two core issues relevant to proper

790 implementation. First, whether to address breach

791 notification separate from broader information security

792 regulation, and second, what burden of proof should be

793 required if a risk-of-harm threshold is adopted for breach

794 notification.

795 I understand the subcommittee to be taking up the issue

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

796 of data security beginning with the question of breach  
797 notification separate from comprehensive information security  
798 regulation. I caution against this approach for two reasons.  
799 First, comprehensive information security combined with  
800 breach notification is substantially more effective than is  
801 either regime alone. As part of my research on information  
802 security regulation, I compared the efficacy of these two  
803 regimes. Specifically of note to the subcommittee's agenda,  
804 the combination of the two was nearly four times more  
805 effective at preventing incidents than was breach  
806 notification alone. I analogize the effects of breach  
807 notification alone to locking the bank or vault door while  
808 leaving a back window wide open.

809         Second, approaching the issue of breach notification  
810 separately requires establishing certain information  
811 categories. For example, defining what information to  
812 protect is essential to breach notification. This  
813 definition, however, has a different purpose when considering  
814 comprehensive information security. Furthermore, once  
815 established, these definitions will be difficult to change.  
816 The burden to business, for example, to reclassify

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

817 information for compliance with multiple definitions is  
818 substantial.

819       To be specific, the types of information that should  
820 trigger notification differ from the types of information  
821 that should be protected overall. For example, medical  
822 records, wills, personal diaries, sensitive or private  
823 photographs and other similar information are all items  
824 federal law currently recognizes as sensitive personal  
825 information. State law has more narrow definitions including  
826 Social Security numbers, financial account number and  
827 government ID numbers. Consumers should be informed about  
828 unauthorized disclosure of all this information. By  
829 contrast, sensitive information about trade secrets, computer  
830 infrastructure or security measures it not the province of  
831 the general consumer, yet such information must also be  
832 secured. On these bases, I strongly recommend that the  
833 subcommittee address breach notification and comprehensive  
834 data security concurrently.

835       The second issue I wish to address is the risk-of-harm  
836 threshold. Certain formulations of this threshold negatively  
837 impact information security. Specifically, a threshold

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

838 employing a negative presumption of notification, which  
839 requires proving risk of harm before triggering notification  
840 requirements, disincentivizes organizations from conducting  
841 thorough investigations. Organizations have incentives to  
842 limit investigations that might increase their liability.  
843 For example, when conducting comprehensive information  
844 security assessments, auditing and consulting firms often  
845 work together with law firms so that the results will be  
846 privileged and thus not discoverable in future civil  
847 litigation or regulatory investigations. Clients do not want  
848 to incur liability for failure to remediate security  
849 vulnerabilities identified in the assessment. A similar  
850 analysis applies to breach investigations. My research data  
851 supports this conclusion as does my professional experience.  
852 Thus, I strongly recommend that if a risk-of-harm threshold  
853 is adopted, the committee adopt an affirmative presumption of  
854 notification where risk of harm must be disproved before  
855 notification is exempted. To place the burden otherwise  
856 disincentivizes information security investigations, one of  
857 the most important tools in protecting consumers against  
858 future breaches and securing the overall information security

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

859 ecosystem.

860 I am happy to offer any assistance to the committee as  
861 it moves forward in his work. I again thank the chairman and  
862 the ranking member for the privilege and opportunity to  
863 testify here today, and I am pleased to answer any of your  
864 questions.

865 [The prepared statement of Mr. Thaw follows:]

866 \*\*\*\*\* INSERT 6 \*\*\*\*\*

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed 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 Mr. {Terry.} Thank you very much for your testimony and  
868 appreciate the two law school professors here. It makes me  
869 feel--I had flashbacks to law school during your testimony.

870 With that, I will start the questions, and it was  
871 fairly--the answer to this is just yes or no, and it was  
872 clearly clear in some of the testimonies but I do want to get  
873 it succinctly on the record starting with Mr. Richards and  
874 then going down to Professor Thaw.

875 Do you believe there should be a federal notification  
876 law? Mr. Richards?

877 Mr. {Richards.} Yes, we do, Mr. Chairman.

878 Mr. {Liutikas.} Yes, we do, Mr. Chairman.

879 Mr. {Greene.} Yes, sir.

880 Ms. {Matties.} Yes.

881 Mr. {Terry.} Now we get to the murkier.

882 Ms. {Matwyshyn.} Exactly. Yes, provided the standard  
883 is at the highest level and does not preempt State law, as  
884 well as conduct being carved out to allow for States to  
885 experiment.

886 Mr. {Thaw.} Yes, provided implemented properly. 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.**

887 provide detail in my written testimony on this, and concur  
888 with Professor Matwyshyn's statement.

889 Mr. {Terry.} See, that is the flashbacks. There is  
890 always enough room to screw up on the test now.

891 Ms. {Matwyshyn.} It always depends, right?

892 Mr. {Terry.} It always depends.

893 And the reason why I think it was important to just lay  
894 that item of foundation is that with 48 States and  
895 territories combined already having at least at the  
896 multinational level, you have a level of sophistication where  
897 they are already in compliance and then there is a level of  
898 concern that a new national standard just creates 49 instead  
899 of 48. So that brings us to what Professor Matwyshyn said in  
900 her ``but'', and that is no State preemption. So how does it  
901 work without preemption, and who wants to start? I will go  
902 with Dr. Matwyshyn first and then anyone else that wants to  
903 speak on preemption.

904 Ms. {Matwyshyn.} So I actually consulted with a  
905 California government official responsible for enforcement,  
906 and provided that the framework on the national level  
907 provides a comprehensive disclosure regime and States 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.**

908 their enforcement agencies have direct access to this  
909 information as well as consumers, everyone wins because the  
910 information would simply be centralized. So if the  
911 disclosure requirements adequately conceptualize the  
912 questions that consumers and enforcers want to know, States,  
913 I believe, would be happy with a centralized regime and there  
914 wouldn't be a problem with enforcement, however, because of  
915 limitations of resources on the part of the Federal Trade  
916 Commission I believe should remain on the State level.

917 Mr. {Terry.} All right. Mr. Richards, Liutikas and  
918 Greene, and Ms. Matties, quickly, though.

919 Mr. {Richards.} Sure. Well, we believe the patchwork  
920 framework occurring in State laws are very duplicative in  
921 some cases, and in a lot of cases don't make sense. North  
922 Dakota, for example, requires notice of a breach of name and  
923 birth date so there are different qualifications in terms of  
924 PII and what information you should focus on. New York  
925 requires notice of security breaches made to three separate  
926 State agencies. I think federal preemption is important but  
927 I don't think you should undermine strong consumer  
928 protections that are currently held and enjoyed at the State

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

929 level.

930 Mr. {Terry.} Thank you. Mr. Liutikas?

931 Mr. {Liutikas.} I mean, at the end of the day I think  
932 we believe that first and foremost that consumers need the  
933 notification standard but in providing that standard, we  
934 could also simplify matters substantially for the small- to  
935 medium-sized business which the current technology  
936 infrastructure allows them to operate in a way that is much  
937 bigger than maybe they could have done some years ago. So I  
938 think centralizing that notification standard and avoiding  
939 having the issue of determining whether or not a variety of  
940 State laws applies or does not apply would be extremely  
941 beneficial to the small- to mid-sized business that simply  
942 doesn't have the resources.

943 Mr. {Terry.} Interesting. Mr. Greene?

944 Mr. {Greene.} I would echo what Mr. Richards said, that  
945 if you have essentially 49 standards, you are just creating  
946 another box you have to check to ensure that you are doing  
947 everything right. If you do have a breach, you are not going  
948 to speed the process of understanding the scope of your  
949 breach of who you need to notify.

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

950           Mr. {Terry.} Thank you. And Ms. Matties, I am actually  
951 going to change the question for you to more personalized  
952 because of your background and experience with the FTC.  
953 There has been a suggestion that at least with some of the  
954 telecoms that the FTC has the experience on data breach and  
955 notification in those areas. If there is a national bill,  
956 should it include the telecommunications and video with the  
957 FTC?

958           Ms. {Matties.} Yes. The FTC has had more than 10 years  
959 of experience working on data breaches and data security  
960 cases, so they are well equipped to handle these kinds of  
961 cases. And I just would like to point out that there is  
962 already a model in Do Not Call for consolidating experiments  
963 in the States with consumer protection. A number of States  
964 have consumer protection laws for Do Not Call in individual  
965 States, and when the national standard became applicable, it  
966 really made things a lot easier for both businesses and for  
967 consumers because now consumers have a one-stop shop to go  
968 and put their name on a list. That would be a similar aspect  
969 here.

970           Mr. {Terry.} All right. Thank you very much.

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

971           The ranking member, Jan Schakowsky, is now recognized  
972 for 5 minutes.

973           Ms. {Schakowsky.} Thank you very much. Mr. Chairman, I  
974 just want to acknowledge that as important as this is to  
975 consumers that maybe in the future we could have a consumer  
976 witness or two to talk about some of their experiences. I  
977 think it would helpful to inform our committee.

978           Talking about data breaches, Professor Matwyshyn, do you  
979 foresee potential harms to the development of effective  
980 information security laws if Congress enacts certain breach  
981 notification provisions without enacting a well-considered  
982 data security law at the same time? I know Professor Thaw  
983 addressed that. And if so, what would they be?

984           Ms. {Matwyshyn.} If I am understanding the question  
985 correctly, I believe that the optimal approach at this  
986 juncture is to bifurcate, to divide off the questions of data  
987 breach notification harm in this Nation from the questions of  
988 the best standard for liability arising from data security  
989 breaches.

990           Ms. {Schakowsky.} To separate those two?

991           Ms. {Matwyshyn.} To separate those two out. While 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.**

992 States have shown us the way and adequately experimented with  
993 notification, the questions of liability, how to craft it,  
994 what the standards are, what reasonable conduct is, that is a  
995 moving target and still very undeveloped, both from the  
996 standpoint of the information security community as a just-  
997 now-coalescing body of experts and from the standpoint of  
998 States having different approaches to consumer protection and  
999 the connection to other bodies of law. The Securities and  
1000 Exchange Commission is starting to regulate in this space.

1001 These issues are tied with broader questions of software  
1002 liability generally, and if we start to regulate too early,  
1003 we may disrupt existing bodies of law and stifle innovation  
1004 that is responsible and consumer protection.

1005 Ms. {Schakowsky.} Okay. I do want to put the same  
1006 question to Professor Thaw and see if the two of you are in  
1007 agreement.

1008 Mr. {Thaw.} I agree with Professor Matwyshyn in the  
1009 respect that the States have the ability to provide important  
1010 experimentation. However, I am concerned about the resources  
1011 that the States have on the technical side. With respect to  
1012 the legal standard, I agree with Professor Matwyshyn. They

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

1013 can experiment and provide us with valuable data. However,  
1014 this is a highly interconnected issue across the entire  
1015 country, and I do not believe that the States have sufficient  
1016 resources for enforcement or for simple providing the  
1017 research and investigation necessary to know what standards  
1018 would be effective at a national level as opposed to at a  
1019 State level.

1020 Ms. {Schakowsky.} Let me get into the issue of data  
1021 brokers. Most consumers have never heard about data brokers  
1022 but there is a several-billion-dollar industry that knows the  
1023 name, address, age, purchasing habits of nearly every  
1024 American consumer. One company in this industry possesses on  
1025 average 1,500 data points apiece on each of 190 million  
1026 individuals in the United States and a profit of more than  
1027 \$77 million on this information. So again, let me go to  
1028 Professor Matwyshyn.

1029 The Data Accountability and Trust Act as was passed in  
1030 the 111th Congress would have required data brokers to submit  
1031 their security policies to the FTC and allow the Commission  
1032 to perform or mandate the performance of security audits  
1033 following a breach of security. What is your opinion 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.**

1034 these kinds of provisions regarding data brokers?

1035 Ms. {Matwyshyn.} In that case, I believe you mentioned  
1036 it was following a breach?

1037 Ms. {Schakowsky.} Yes.

1038 Ms. {Matwyshyn.} That would be entirely consistent with  
1039 the types of proposals that we are considering now for  
1040 centralized breach notification. The goal is to get as much  
1041 information about breaches, how they happened, why they  
1042 happened, the level of security that is in place in the  
1043 particular organization to provide the information to both  
1044 consumers and enforcement agencies to determine which  
1045 entities are the good actors and which entities are the  
1046 actors that still have a way to go to improve the level of  
1047 care.

1048 Ms. {Schakowsky.} With just a minute or two, actually  
1049 less than that, you may also want to comment on data brokers  
1050 and the role that they play and how they should be regulated,  
1051 Professor Thaw?

1052 Mr. {Thaw.} With respect to data brokers, I draw the  
1053 committee's attention to the fourth section of my written  
1054 testimony where I identify different levels of criticality,

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

1055 and I would suggest that data brokers are at a higher level  
1056 of criticality, the reason being that the information they  
1057 contain, to use Professor Matwyshyn's earlier example, could  
1058 be information which is an authentication credential such as  
1059 your mother's maiden name or your favorite color, your first  
1060 pet, something that you use to secure other data that is very  
1061 sensitive. For this reason, they should be regulated at a  
1062 higher level, and this is something that cannot be  
1063 overlooked.

1064 Mr. {Terry.} Thank you, and now we recognize the  
1065 chairman emeritus for 5 minutes.

1066 Mr. {Barton.} Thank you, Mr. Chairman. I am going to  
1067 try to give you a little bit of that time back.

1068 I think in your questions, Mr. Chairman, we established  
1069 the panel does support a federal standard for notification.  
1070 My question would be, does the panel also support going  
1071 beyond that so that we get into the prevention and the  
1072 liability issues? Does everybody, you know, support a  
1073 federal law that goes beyond breach notification?

1074 Mr. {Richards.} I think that would depend on--we would  
1075 obviously have to see the legislation but I certainly think

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

1076 we should probably change the culture of how our society  
1077 looks at cybersecurity or information technology and how do  
1078 you protect the information. Instead of making it an IT  
1079 department issue, make it a CFO issue and really change the  
1080 thinking and the approach to how we approach data protection  
1081 in the country.

1082 Mr. {Liutikas.} I think we also need to look to  
1083 industry associations like CompTIA which provides the  
1084 industry a platform for collaborating on standards and best  
1085 practices and their industry credentials such as the CompTIA  
1086 Security Trust Mark credential, which audits the security  
1087 practices of an organization. So I think in light of  
1088 considering options such as that, I think we should also look  
1089 at the options that the industry can provide as well.

1090 Mr. {Greene.} Conceptually, you know, we support the  
1091 notion of requiring security standards, so you are looking to  
1092 prevent the breach, not just to mitigate after, and the same  
1093 thing with the encryption. So if you have a breach, you are  
1094 limiting the damage that can happen. But as Mr. Liutikas  
1095 said, there are a lot of existing industry standards that are  
1096 effective, and any type of standard needs to be very flexible

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

1097 and performance based. We don't want to be mandating  
1098 anything specific in statute when we have a very shifting  
1099 threat environment. So the notion of saying you need to be  
1100 secure is okay, but if we get into the where we are mandating  
1101 specific types of solutions, I think that could be  
1102 problematic.

1103 Ms. {Matties.} CTIA members and the broader 21st  
1104 Century Privacy Coalition is interested in talking about data  
1105 security for sure but we are happy to see that we are  
1106 starting with data breach notifications.

1107 Ms. {Matwyshyn.} No limitations of liability are  
1108 appropriate at this juncture. I think we are a little too  
1109 premature. On the State level, experimentation would be  
1110 great. A negligence standard perhaps evolving would be a  
1111 good move. I think we are ready to address breach  
1112 notification but I would be cautious in approaching  
1113 liability.

1114 Mr. {Thaw.} Yes, if properly implemented, and I note  
1115 that respectfully, Mr. Richards, I am concerned with his  
1116 proposal of making this a CFO issue. While that is  
1117 appropriate to companies' fiduciary duties under State law,

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

1118 it is not appropriate to the question of negative  
1119 externalities that would result from breaches in one  
1120 organization to the overall information ecosystem. I also do  
1121 concur with my panelists' opinion that flexible standards are  
1122 important.

1123 Mr. {Barton.} I agree with flexible standards.

1124 Mr. Chairman, I want to turn it back, but let me simply  
1125 say, back in the 1930s when we had a rash of kidnappings, the  
1126 Congress did not pass a kidnapping notification law. They  
1127 passed strict laws delineating it was a federal crime if it  
1128 crossed State lines and empowered the FBI to use every means  
1129 possible to go after the kidnappers. We are not talking  
1130 about stealing our children but we are talking about stealing  
1131 our identifies, and I would hope that this subcommittee and  
1132 the full committee goes beyond breach notification law, and  
1133 with that, I yield back.

1134 Mr. {Terry.} It is the intent. I am going to call on  
1135 Mr. Barrow, and then we will adjourn, so if you are next in  
1136 line as a Republican, you can go to the meeting.

1137 Mr. Barrow, you are now recognized for 5 minutes.

1138 Mr. {Barrow.} Thank you, Mr. Chairman, and 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.**

1139 for setting the table with your questions. I want to follow  
1140 up some of the issues that you raised.

1141 You know, privacy is important to me. The right to be  
1142 secure in your persons and papers from State intrusion is in  
1143 the Fourth Amendment. Warren and Brandeis said that the  
1144 right to be let alone, the right of privacy is the right most  
1145 prized by civilized men, I guess we would say today civilized  
1146 men and women. I certainly agree with them on that.

1147 I guess the general consensus is that the current regime  
1148 of essentially 48 separate State and territorial  
1149 jurisdictions regulating this matter and our common market of  
1150 the United States just ain't working. I think we all agree  
1151 with that, and there is a general need for some federal  
1152 guidelines, some federal standards for a uniform law in our  
1153 national economy.

1154 Mr. Richards, Mr. Liutikas, Ms. Matties, you each talk  
1155 about the subject of preemption, the need to preempt  
1156 conflicting State laws. I want to ask the other members of  
1157 the panel, what is the appropriate scope of federal  
1158 preemption in this area? Yes, ma'am, go ahead.

1159 Ms. {Matwyshyn.} I believe the appropriate scope 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.**

1160 creating a harmonized disclosure form but enforcement should  
1161 be shared in the same way that it is in securities  
1162 regulation. In the securities regulation context, we have  
1163 multiple sources of oversight--the FCC, State level,  
1164 securities regulators, other agencies inside the States.

1165 Mr. {Barrow.} Are you proposing a uniform law but  
1166 shared responsibility with respect to enforcing the same law  
1167 so the federal regulator would set the rules and regulations  
1168 but the State folks might enforce the same federal law if the  
1169 federal government isn't devoting enough resources to  
1170 enforcing its law, the national standard? Is that what you  
1171 have in mind?

1172 Ms. {Matwyszyn.} In the same way that securities  
1173 disclosures happen on the federal level primarily but a  
1174 particular State may have requirements in terms of protecting  
1175 its citizens.

1176 Mr. {Barrow.} Well, additional requirements, additional  
1177 substantive regulations and obligations and duties is  
1178 different from a uniform standard that either the federal  
1179 prosecutor or the State prosecutor can enforce the same law--  
1180 one land, one law. That is a very different matter. 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.**

1181 having the right at the State level to enforce a federal  
1182 standard is different than being able to make your own  
1183 standard and enforce that in addition to the federal  
1184 standard, so I want to talk about whether or not there are  
1185 other folks on the panel who agree with the proposition that  
1186 federal regulation ought to occupy the field when it comes to  
1187 the substantive obligations and responsibilities in this  
1188 area. Mr. Greene?

1189 Mr. {Greene.} Sir, we would agree that it should occupy  
1190 the field but ultimately I think the notion of State  
1191 enforcement would be acceptable as long as we are talking  
1192 about a uniform federal standard.

1193 Mr. {Barrow.} I got you.

1194 Professor Thaw?

1195 Mr. {Thaw.} State enforcement concurrent with federal  
1196 enforcement would be appropriate, and I want to emphasize  
1197 that in either case, centralized notification and collection  
1198 by a federal regulator so that we have information on what is  
1199 going on is critical.

1200 Mr. {Barrow.} All right. We have had a slight  
1201 diversity of opinion with respect to who ought to be able 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.**

1202 make the rules, but there seems to be a general consensus  
1203 that as long as we are enforcing the same rules, it doesn't  
1204 matter which government the cop reports to if they are  
1205 enforcing the law.

1206 I want to get to the subject of who ought to be the  
1207 federal regulator. I think, Ms. Matties, you said that we  
1208 not only need to have a uniform federal system but it ought  
1209 to be headed up by the FTC as opposed to, say, the FCC. Does  
1210 anybody disagree with that on the panel as to which federal  
1211 regulator ought to be making the rules that we will be trying  
1212 to enforce on a consistent basis nationwide? Does anybody  
1213 disagree with that approach? Professor Thaw?

1214 Mr. {Thaw.} I agree that the Federal Trade Commission  
1215 is the most appropriate for consumer regulation. However,  
1216 that should not exempt critical infrastructure providers,  
1217 which would include telecommunications providers from  
1218 regulations to which they would also be subject by their  
1219 regulators. Those regulators, for example, the Federal  
1220 Communications Commission, the Nuclear Regulatory Commission  
1221 are better familiar with what are the challenges faced by  
1222 their entities, and if they need to impose additional

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

1223 standards, they should not be prevented from doing so by  
1224 consumer regulation.

1225 Mr. {Barrow.} Is it your position that they can  
1226 regulate in their areas of subject-matter jurisdiction and  
1227 should not be able to regulate in the area of consumer  
1228 protection?

1229 Mr. {Thaw.} If I understand your question correctly, my  
1230 position is not that they should be pushing out the consumer  
1231 regulator so the consumer regulator has no authority but only  
1232 that they may and if necessary should regulate concurrently  
1233 with the consumer regulator.

1234 Mr. {Barrow.} What do other members of the panel feel  
1235 about that? Mr. Richards, Mr. Liutikas, Mr. Greene?

1236 Mr. {Richards.} Mr. Barrow, I would say that the FTC  
1237 definitely when it comes to consumer information certainly I  
1238 think our approach to privacy in this country is somewhat  
1239 patchwork when you are dealing with HIPAA and the Fair Credit  
1240 Reporting and Gramm-Leach-Bliley, so I certainly think that  
1241 the current functional regulators also have a good system in  
1242 place but the FTC certainly is equipped when it comes to  
1243 consumer information.

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

1244 Mr. {Barrow.} Mr. Liutikas?

1245 Mr. {Liutikas.} I would generally concur with that  
1246 although I think we would have to conduct some further  
1247 analysis and see what really makes sense at the end of the  
1248 day. You know, the question right now is somewhat  
1249 theoretical but I think overall makes sense, and we certainly  
1250 support having a federal agent, so whichever department that  
1251 is.

1252 Mr. {Barrow.} Well, my time has run out, Mr. Greene. I  
1253 regret that. But if any of you all want to follow up on this  
1254 and supplement the responses that you have given or that  
1255 others have given on this subject, please feel free to do so  
1256 for the record.

1257 Thank you so much, and thank you, Mr. Chairman.

1258 Mr. {Terry.} And I mistakenly used the word ``adjourn''  
1259 earlier. We are recessing until probably 1 o'clock,  
1260 hopefully by 1:03 or 1:04 we are asking questions of you. So  
1261 thank you for your patience, and we will see you in 50, 55  
1262 minutes.

1263 [Recess.]

1264 Mr. {Terry.} I appreciate you all being back. We 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.**

1265 missing Professor Thaw for the moment.

1266 Ms. {Matwysyn.} He went to go fetch a deserted bag so  
1267 that they don't confiscate it. He will be right back.

1268 Mr. {Terry.} Oh, that is important. We will string  
1269 things out, but we will start with the questions. We have a  
1270 short time before either votes or the next committee takes  
1271 over. So we don't want to delay until he comes back but we  
1272 will start with other people.

1273 Vice Chairman of the subcommittee, you are recognized  
1274 for 5 minutes, Mr. Lance.

1275 Mr. {Lance.} Thank you, Mr. Chairman, and good  
1276 afternoon to the panel.

1277 To Ms. Matties, what, in your opinion, should be the  
1278 proper standard for breach notification? Suspicion that a  
1279 breach has occurred or actual evidence that such a breach has  
1280 occurred?

1281 Ms. {Matties.} Actual evidence that a breach has  
1282 occurred.

1283 Mr. {Lance.} So you would have a higher standard  
1284 before--

1285 Ms. {Matties.} Yes.

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

1286           Mr. {Lance.} Thank you. And number two, should a  
1287 breach have to result in identity theft or other financial  
1288 harm to require consumer notification?

1289           Ms. {Matties.} There certainly should be consumer  
1290 notification for identify theft and financial harm, and we  
1291 are willing to talk to you about the other kinds of harms  
1292 that might result from a breach of other information.

1293           Mr. {Lance.} Do you have suggestions regarding that  
1294 other than financial harm?

1295           Ms. {Matties.} We are still working with our members to  
1296 talk about this, and we look forward to talking to you as  
1297 well about it.

1298           Mr. {Lance.} Thank you.

1299           Are there others on the panel who have an opinion on  
1300 that? Yes, Professor.

1301           Ms. {Matwyshyn.} I believe that actual harm should not  
1302 be required for notification. It serves a function to advise  
1303 consumers of the occurrence of a breach and also to allow for  
1304 tabulation and centralization of information about security  
1305 practices so that we can collectively get a better picture of  
1306 the entirety of the economy and the behaviors that 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.**

1307 happening around information security.

1308 Mr. {Lance.} Thank you.

1309 Others on the panel? Mr. Richards?

1310 Mr. {Richards.} I thank you. We would--our standard  
1311 would be that there should be a notification requirement if  
1312 the breach presents a significant risk of harm to consumers  
1313 and may perpetuate identity theft.

1314 Mr. {Lance.} A significant harm to consumers, which  
1315 might be a slightly different standard from financial harm,  
1316 if I am understanding you accurately?

1317 Mr. {Richards.} Yes.

1318 Mr. {Lance.} Professor Thaw?

1319 Mr. {Thaw.} I believe that notification should at least  
1320 occur in all cases to a central reporting authority, which  
1321 could be a federal regulator, that a substantial risk of harm  
1322 is too high a threshold. I base this on the civil litigation  
1323 where it was virtually impossible for any case to advance  
1324 based on those types of claims, and with respect to the types  
1325 of harm, I believe this requires further investigation but  
1326 should not be limited to identity theft.

1327 Mr. {Lance.} And if the notification were made to an

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

1328 entity of the federal government, that entity would then in  
1329 turn determine whether further notification should be made to  
1330 the consumer?

1331 Mr. {Thaw.} That would be conditional on whether or not  
1332 notification had already been made also by the company. I  
1333 think at least the agency should retain the right to make  
1334 that determination.

1335 Mr. {Lance.} Thank you. Are there other thoughts from  
1336 the panel? Hearing none, Mr. Chairman, I am finished with 2  
1337 minutes to.

1338 Mr. {Terry.} Thank you, Mr. Lance.

1339 Mr. Harper, you are now recognized for 5 minutes.

1340 Mr. {Harper.} Thank you, Mr. Chairman, and thank each  
1341 of you for being here, and it is a very important issue to  
1342 each of you, I know, and certainly it is to our country and  
1343 many businesses, and I will start with you, if I could, Mr.  
1344 Richards, and ask you, how would you define a breach that  
1345 constitutes a reasonable risk of harm to consumers?

1346 Mr. {Richards.} Sure. Thank you, Congressman. In  
1347 terms of a reasonable risk, we believe that data that could  
1348 be used to perpetuate identity theft, if you were to allow

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

1349 someone to use, log in to or access an individual's account  
1350 or establish a new account using that individual's  
1351 identifying information, and we would hold it to that  
1352 standard.

1353 Mr. {Harper.} So as you define a breach, how do you  
1354 define a significant risk of harm to consumers?

1355 Mr. {Richards.} If there is a risk of identity theft or  
1356 stealing personal information and using or creating a new  
1357 identity based on that personal information.

1358 Mr. {Harper.} Well, how should we or how would we  
1359 define what constitutes a significant risk of harm to  
1360 consumers? If you were advising us, if Congress did define  
1361 the type of personally identifiable information that  
1362 constitutes harm to consumers, is it possible that such a  
1363 list would keep up with technological innovations?

1364 Mr. {Richards.} Yes, sir. I think it is important not  
1365 to mandate specific technologies. As you know, we need a  
1366 flexible framework. Some technologies today and best  
1367 practices can render data useless, and in that case, if a  
1368 company or an organization is trying to take the right  
1369 approach and render the data useless, we believe a safe

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

1370 harbor should be granted to incentivize that good behavior if  
1371 the information is indecipherable, but we need a flexible  
1372 framework in an effort not to undermine innovation for new  
1373 technologies that come down the line.

1374 Mr. {Harper.} And I know I am going to mispronounce  
1375 your name, Ms. Matties, if I could ask you a question. My  
1376 understanding from your testimony is that different data  
1377 breach requirements apply to different entities, even for the  
1378 same information. Is there any public policy justification  
1379 for applying different data breach requirements to the same  
1380 information?

1381 Ms. {Matties.} No, there is not.

1382 Mr. {Harper.} And I will ask this panel-wide, if I  
1383 could. All of your testimony points out that States have  
1384 different notification requirements and definitions. Is  
1385 there a certain time frame post breach that you believe  
1386 individuals have a right to be notified? I would like to  
1387 hear each of your responses on that, and I will start with  
1388 you, Mr. Richards.

1389 Mr. {Richards.} Certainly. Well, we think there needs  
1390 to be a little bit of time in order for a company to perform

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

1391 cyber forensics. We don't have a specific position on a  
1392 specific time frame but our businesses and their approach is  
1393 as quickly as possible and consulting with law enforcement  
1394 and others, and we follow up on our due diligence and report  
1395 it to the consumer as quickly as possible.

1396 Mr. {Harper.} Well, following up on that, how can--  
1397 maybe you can walk me through. How is notification without  
1398 unreasonable delay how that really works in the real world?

1399 Mr. {Richards.} Well, I think in terms of, if you look  
1400 at the different State requirements, there is different time  
1401 frames that are offered. Puerto Rico is 10 days to notify  
1402 folks. Vermont is about 14 days. Minnesota requires  
1403 reporting to credit bureaus within 48 hours. So sometimes  
1404 when you are looking at the condensed time frame, you are  
1405 really trying to figure out the extent of the breach, what  
1406 has been breached. So I think in terms of those time frames,  
1407 it is a very short turnaround and a very short fuse, and I  
1408 think companies want to make sure that they have the right  
1409 answers before they disclose information publicly but I  
1410 believe they do have the responsibility to report it to  
1411 consumers.

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

1412           Mr. {Harper.} Thank you. And I will ask each of you,  
1413 is there a certain time frame post breach that you believe  
1414 individuals have a right to be notified?

1415           Mr. {Liutikas.} Yes, Congressman, we certainly--and we  
1416 will mirror a little bit of what Mr. Richards said. We  
1417 believe in a reasonable time frame in which to notify. I  
1418 think it is just important for the exceptions to be made for  
1419 instances where law enforcement needs to act or other  
1420 information needs to be gathered so that the correct  
1421 information is being provided to the consumers. So we don't  
1422 have an exact timeline that we recommend but we do recommend  
1423 having exceptions for those legitimate reasons.

1424           Mr. {Harper.} And Mr. Greene, I think I can at least  
1425 get your response before my time is up.

1426           Mr. {Greene.} Sure. I would say that you definitely  
1427 need to have enough time so the company can determine the  
1428 scope of what was lost and what wasn't lost, fix the  
1429 vulnerability. You don't want to go public and basically  
1430 hang a target around your neck, and I would say, though, a  
1431 rush to report can be bad. Every incident is different. I  
1432 think if there is one rule, it is that first reports 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.**

1433 pretty much always wrong. With respect to the breach about  
1434 Congress today, you are going to see what was published today  
1435 a week from now is going to be outdated, is going to be  
1436 different, so you need to allow time. It needs to be as  
1437 quickly as possible but you need to make sure that you are  
1438 getting it right. It is better to be right in most cases  
1439 than it is to be fast.

1440 Mr. {Harper.} Thank you, and I believe my time has  
1441 expired so I yield back, Mr. Chairman.

1442 Mr. {Terry.} Thank you, and now the chair recognizes  
1443 the gentleman from Texas, of which he is very proud and will  
1444 probably mention that. He is recognized for 5 minutes.

1445 Mr. {Olson.} Thank you, Mr. Chairman, for holding this  
1446 hearing, and thank you to the witnesses for attending.

1447 Mr. Chairman, you should know that I got my plug in with  
1448 all the witnesses as to why they should move to the great  
1449 State of Texas before we were gaveled in at 11 o'clock, so we  
1450 are done with that business.

1451 At the end of the day, this hearing, to me, is about two  
1452 questions. Number one, is federal legislation necessary when  
1453 data has been breached. If the answer is yes, then what

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

1454 should that legislation look like. In your written  
1455 testimonies as I reviewed it last night, it appears that  
1456 federal legislation would help protect consumers, but Mr.  
1457 Richards raises the point that there are some technology  
1458 companies it is helpful but not vital. The two professors  
1459 were concerned with, you know, federal government overreach  
1460 and taking over what the States are doing pretty well. But I  
1461 believe this difference raises an important point, that if we  
1462 pursue legislation, we must carefully draft it to ensure that  
1463 the federal government doesn't become the 49th entity out  
1464 there that companies must comply with. We should have a  
1465 Hippocratic oath for data breaches: harm has been done; do  
1466 no more harm.

1467 In regards to the ultimate decision to pursue  
1468 legislation, consumers expect their privacy of their personal  
1469 information to be protected, and I know you all agree we must  
1470 keep them at the forefront of this conversation and debate.

1471 My first question is for you, Ms. Matties. Do you think  
1472 the existence of 48 different data breach regimes results in  
1473 brief notifications being faster or slower?

1474 Ms. {Matties.} I think it makes it slower. Companies

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

1475 try very hard to comply with all the laws out there but it  
1476 certainly is a distraction, at best, from the other tasks  
1477 that they need to complete when dealing with a data breach as  
1478 has been discussed by the other panelists.

1479 Mr. {Olson.} Does anybody else care to comment on that,  
1480 faster or slower? Professor Thaw?

1481 Mr. {Liutikas.} Congressman, I think it makes it  
1482 significantly--oh, I apologize.

1483 Mr. {Olson.} You are up next, Mr. Liutikas.

1484 Mr. {Thaw.} I believe historically it has made it  
1485 slower but it absolutely does not need to. It is a very  
1486 formulaic regime for which procedures can be developed, for  
1487 example, to analogize to something with which I believe many  
1488 people may be familiar, Legal Zoom, the product that  
1489 provides--you punch in the information, we generate a will or  
1490 something similar. I could develop today a program that  
1491 would handle the current jurisdiction requirements in place.

1492 Mr. {Olson.} Okay, Mr. Liutikas, come on in.

1493 Mr. {Liutikas.} Thank you, Congressman. In addition to  
1494 making the process slower today, I think the process of  
1495 actually evaluating all of the different requirements 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.**

1496 laws out there also creates more opportunity for not properly  
1497 reporting under a variety of State laws. So not only does it  
1498 slow it down, I think there is more opportunity for mistakes  
1499 to be made as well.

1500 Mr. {Olson.} Thank you.

1501 Another one for you, Ms. Matties. How do wireless  
1502 companies deal with the fact that States have different  
1503 definitions of personal information? Can that result in  
1504 over-reporting in some States? Does it create consumer  
1505 confusion? And what harm may companies incur if they over-  
1506 report and some examples? So basically over-reporting,  
1507 confusion, harm, examples.

1508 Ms. {Matties.} I am not sure I have examples for all  
1509 those questions, but certainly, over-reporting can be a  
1510 problem. It is sort of the boy who cried wolf. If you get  
1511 notices over and over that actually don't pertain to you, you  
1512 may start to ignore them, but worse, you may actually start  
1513 making changes to your passwords and closing and opening bank  
1514 accounts unnecessarily, wasting your own energy. So the  
1515 different State regimes can cause over-reporting, which can  
1516 harm consumers, and it also certainly impacts businesses 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.**

1517 being able to comply with those laws.

1518 Mr. {Olson.} It looks like the professor wants to make  
1519 comments. Ma'am, you are up.

1520 Ms. {Matwyszyn.} I wanted to play up on that point.  
1521 The two complaints--I shouldn't say complaints. The two  
1522 comments that I have heard repeatedly from businesses in  
1523 their compliance efforts, first, that the regulatory end of  
1524 this complicated. Different regulators are required to  
1525 receive filings in different States so simplifying the  
1526 regulatory complexity would be something they would want.

1527 The second point that they repeatedly mention to me is  
1528 the definition of what constitutes information that triggers  
1529 reporting, and they would be happy with a broader definition  
1530 of the information that triggers information as long as it is  
1531 a bright line, it is clear to them. And so many companies,  
1532 especially the most sophisticated technology companies, are  
1533 now erring on the side of reporting because it is simpler,  
1534 and they don't view it necessarily as a bad thing, they just  
1535 want simplification and a single regulatory point of contact.

1536 Mr. {Olson.} And i would assume when they go public  
1537 that they have had some data breach, that affects their

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

1538 business because consumers look at a company that has had a  
1539 data breach, maybe is having some faults, which is not true,  
1540 but the bottom line, in the market they get spooked and move  
1541 their products elsewhere. One more comment, ma'am. I am out  
1542 of time.

1543 Ms. {Matwyshyn.} If I can just follow up, the other  
1544 benefit that a centralized point provides is the ability for  
1545 companies engaging in highest security practices to announce  
1546 that. So even if they suffer a data breach from a zero day  
1547 vulnerability, for example, if they are using the highest-end  
1548 software possible, then enforcement agencies are going to say  
1549 oh, they tried really hard, this is a good company doing the  
1550 right thing. But if it is someone who hasn't updated their  
1551 systems in 6 years and that is why they had a data breach,  
1552 that is a completely different ball of wax.

1553 Mr. {Olson.} I am out of time. I thank the witnesses,  
1554 and come to Texas.

1555 I yield back.

1556 Mr. {Terry.} No.

1557 Mr. Johnson, you are recognized.

1558 Mr. {Johnson.} Also no, Mr. Chairman.

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

1559 I would like to thank the panel for being here today. I  
1560 spent about 30 years of my professional career before I came  
1561 to Congress in the information technology field in the  
1562 Department of Defense, worked as the director of the CIO  
1563 staff for special operations command, so I certainly  
1564 understand the complexities of data security and how easy it  
1565 is for those who are determined to get into it

1566 So with that as a backdrop, do we have any empirical  
1567 data to answer the question about how quickly we should  
1568 notify consumers? I mean, do we have any data that tells us  
1569 after several hundred thousand identities are breached, do we  
1570 know how long before the bad guys start using that  
1571 information? Anybody on the panel? Mr. Greene?

1572 Mr. {Greene.} Unfortunately, there is no answer. There  
1573 are thriving black markets in personal information, whether  
1574 it is a Social Security number, et cetera, or simply credit  
1575 card numbers, and it can be a game of roulette whether your  
1576 card is bought before it goes stale or not, so we don't know  
1577 how fast. It really depends on how they are going to use  
1578 their information. Slightly off point, but there is  
1579 empirical evidence. The Ponemon study from last year found--

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

1580 it was looking at the impacts, and one of the drivers of  
1581 increased costs was notification too early. What they found  
1582 is, companies that rushed to notify often notified a  
1583 significant number of people who once they did their full  
1584 forensic work had not actually had their personal information  
1585 made public, yet the companies notified them. The  
1586 individuals, many of them, went to the trouble of changing  
1587 passwords, etc. The company had to pay for monitoring and  
1588 other services. So we do know--and again, not discounting  
1589 the need to notify quickly but doing it too quickly can drive  
1590 up costs, both for the individuals and the companies.

1591 Mr. {Johnson.} Speaking of quickly or not quick enough,  
1592 do you think that breaches are over- or under-notified today?  
1593 Again for the entire panel. Does anybody have a thought?  
1594 Yes, ma'am.

1595 Ms. {Matwyshyn.} I would say they are dramatically  
1596 under-notified. Frequently, they are never discovered, and  
1597 that is partially because companies unfortunately don't  
1598 always have state-of-the-art security in the place. Also in  
1599 the public sector, we have the same challenges with security.  
1600 So I would assume there are two breaches for every one 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.**

1601 is reported.

1602 Mr. {Johnson.} Given that there is a plethora of State  
1603 regulations that require this, do you think an overarching  
1604 federal standard lessens the risk of under- or over-  
1605 notification?

1606 Ms. {Matwyshyn.} I think it is heading in the right  
1607 direction. I think we are improving. We are all becoming  
1608 more educated about these issues. Companies are becoming  
1609 more sensitive. There is dramatic improvement in the last  
1610 decade, and particularly in industries such as financial  
1611 services, they are improving, and there is a learning curve  
1612 happening, so we are heading in a good direction, and I think  
1613 federal harmonized legislation is a step in that direction.

1614 Mr. {Johnson.} Mr. Richards, you noted that the FTC has  
1615 been relatively active in bringing cases against companies  
1616 for failure to maintain or disclose their security practices.  
1617 If the FTC has this existing authority, do we need to address  
1618 data security in more federal legislation?

1619 Mr. {Richards.} Congressman, in reference to your last  
1620 point, I believe strong federal preemptive data breach  
1621 notification law that is broad in scope would cut down 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.**

1622 over-notification certainly. We believe that the FTC does  
1623 have a lot of jurisdiction within its existing authority but  
1624 we believe given the patchwork quilt of 48 different State  
1625 laws that a broad federal preemptive law would be very  
1626 helpful to our businesses.

1627 Mr. {Johnson.} Well, I think I know the answer to this  
1628 next question, Mr. Richards, but can data security and data  
1629 breach notification be addressed separately or are they hand  
1630 in hand?

1631 Mr. {Richards.} Well, I think they can be. Well, I  
1632 would suggest addressing them separately, first data breach  
1633 notification, getting some consensus on the committee. I  
1634 think certainly the conversation around data security is  
1635 important. I think there should be some focus on what we  
1636 have been talking about in terms of a safe harbor, how do you  
1637 incentivize companies or give companies some type of guidance  
1638 on how they render the data useless so if it is hacked or  
1639 stolen, you have taken the measures and you shouldn't have to  
1640 report. So I think certainly as a balance, a lot of the  
1641 focus has been on what happens post breach but I certainly  
1642 think there are some measures they can take pre 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.**

1643 Mr. {Johnson.} Great. I think I am last, Mr. Chairman.

1644 If you would indulge for one more?

1645 Mr. Greene, you stated that there were 93 million  
1646 identities exposed in 2012. Does this mean people, their  
1647 names, their user names or their Social Security numbers?  
1648 Why does identity mean in that 93 million number?

1649 Mr. {Greene.} By the way we counted, it was name in  
1650 connection with Social Security number, address--one of the  
1651 following: Social Security number, address, date of birth or  
1652 credit card information. Essentially, information that put  
1653 together would allow financial fraud or identity theft.

1654 Mr. {Johnson.} All right. Thank you, Mr. Chairman. I  
1655 yield back.

1656 Mr. {Terry.} Well done, everybody, so that concludes  
1657 the questioning period, which means that we are finished  
1658 except for a little bit of work here.

1659 I ask unanimous consent to include the following  
1660 statements in the record: one, statement of the Electronic  
1661 Transaction Association dated July 18, 2013; two, a letter  
1662 from the Credit Union National Association, CUNA, dated July  
1663 17, 2013; a letter from McDonald Hopkins LLC dated July 18,

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

1664 2013; number four, National Retail Federation statement dated  
1665 July 18, 2013. These have all been approved by the minority  
1666 staff. Hearing no objections then, so ordered.

1667 [The information follows:]

1668 \*\*\*\*\* 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.**

|  
1669           Mr. {Terry.} No documents to be submitted on your side.  
1670 Now all of our business is done, and I want to thank all of  
1671 you. It has been very insight. It was very stimulating, and  
1672 we greatly appreciate your time and your testimony, which is  
1673 your talent, and thank you, and we are adjourned.  
1674           [Whereupon, at 1:24 p.m., the Subcommittee was  
1675 adjourned.]