

**This is a preliminary transcript of a Committee hearing. It has not yet been subject to a review process to ensure that the statements within are appropriately attributed to the witness or member of Congress who made them, to determine whether there are any inconsistencies between the statement within and what was actually said at the proceeding, or to make any other corrections to ensure the accuracy of the record.**

1 {York Stenographic Services, Inc.}

2 RPTS ALDINGER

3 HIF153.170

4 HEARING ON ``SONY AND EPSILON: LESSONS FOR DATA SECURITY

5 LEGISLATION''

6 THURSDAY, JUNE 2, 2011

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 12:05 p.m.,  
12 in Room 2123 of the Rayburn House Office Building, Hon. Mary  
13 Bono Mack [Chairwoman of the Subcommittee] presiding.

14 Members present: Representatives Bono Mack, Blackburn,  
15 Stearns, Harper, Lance, Guthrie, Olson, McKinley, Pompeo,  
16 Kinzinger, and Butterfield.

17 Staff present: Charlotte Baker, Press Secretary; Allison  
18 Busbee, Legislative Clerk; Paul Cancienne, Policy

19 Coordinator, Commerce, Manufacturing and Trade; Brian  
20 McCullough, Sr. Professional Staff Member, Commerce,  
21 Manufacturing and Trade; Gib Mullan, Chief Counsel, Commerce,  
22 Manufacturing and Trade; Shannon Weinberg, Counsel, Commerce,  
23 Manufacturing and Trade; Michelle Ash, Democratic Chief  
24 Counsel; Felipe Mendoza, Democratic Counsel; and Will  
25 Wallace, Democratic Policy Analyst.

|  
26           Mrs. {Bono Mack.} Good afternoon. If the room would  
27 please come to order. Guests, kindly take your seats. Thank  
28 you. So good afternoon.

29           In today's online world, your name, birth date, and  
30 mother's maiden name are often used to verify your identity.  
31 But in the wake of massive data breaches at Sony and Epsilon,  
32 we are now painfully more aware that this very same  
33 information can be used just as easily to falsify your  
34 identity. The time has come for Congress to take action.  
35 And the chair now recognizes herself for an opening  
36 statement.

37           With nearly 1.5 billion credit cards now in use in the  
38 United States and more and more Americans banking and  
39 shopping online, cyber thieves have a treasure chest of  
40 opportunities today to get rich quick. Why crack a vault  
41 when you can hack a network? The Federal Trade Commission  
42 estimates that nearly 9 million Americans fall victim to  
43 identity theft every year, costing consumers and businesses  
44 billions of dollars annually, and those numbers are growing  
45 steadily and alarmingly.

46           In recent years, sophisticated and carefully  
47 orchestrated cyber attacks designed to obtain personal  
48 information about consumers, especially when it comes to

49 their credit cards, have become one of the fastest-growing  
50 criminal enterprises here in the U.S., as well as across the  
51 world. Just last month, the Justice Department shut down a  
52 cyber crime ring believed to be based in Russia, which was  
53 responsible for the online theft of up to \$100 million.

54 The boldness of these attacks and the threat they  
55 present to unsuspecting Americans was underscored recently by  
56 massive data breaches at Epsilon and Sony. In some ways,  
57 Sony has become Ground Zero in the war to protect consumers'  
58 online information. The initial attacks on Sony's  
59 PlayStation network and online entertainment services, which  
60 put some 100 million customer accounts at risk, were quickly  
61 followed by still more attacks at other Sony divisions and  
62 subsidiaries. Since then, the company, to its credit, has  
63 taken some very aggressive steps to prevent future cyber  
64 attacks such as installing new firewalls, enhancing data  
65 protection, and enhancing their encryption capabilities,  
66 expanding automated software monitoring, and hiring a new  
67 chief information security officer.

68 These are all important new safeguards, but with  
69 millions of American consumers in harm's way, why weren't  
70 these safety protocols already in place? For me, one of the  
71 most troubling issues is how long it took Sony to notify  
72 consumers and the way in which the company did it--by posting

73 an announcement on its blog. In effect, Sony put the burden  
74 on consumers to search for information instead of providing  
75 it to them directly. That cannot happen again.

76 While I remain critical of Sony's initial handling of  
77 these data breaches, as well as its decision not to testify  
78 at our last hearing--and that goes for Epsilon as well--it is  
79 clear that since then, the company has been systematically  
80 targeted by hackers and cyber thieves who are constantly  
81 probing Sony's security systems for weaknesses and  
82 opportunities to infiltrate its networks.

83 So today, I am not here to point fingers. Instead, let  
84 us point the way, a better, smarter way to protect American  
85 consumers online. As I have said, you shouldn't have to  
86 cross your fingers and whisper a prayer whenever you type in  
87 a credit card number on your computer and hit ``Enter.'' E-  
88 commerce is a vital and growing part of our economy. We  
89 should take steps to embrace and protect it and that starts  
90 with robust cyber security.

91 As chairman of the subcommittee, I believe the lessons  
92 learned from the Sony and Epsilon experiences can be  
93 instructive. How did these breaches occur? What steps are  
94 being taken to prevent future breaches? What is being done  
95 to mitigate the effects of these breaches? And what policies  
96 should be in place to better protect American consumers in

97 the future. Most importantly, consumers have a right to know  
98 when their personal information has been compromised, and  
99 companies have an overriding responsibility to promptly alert  
100 them. These recent data breaches only reinforce my long-held  
101 belief that much more needs to be done to protect sensitive  
102 consumer information.

103 Americans need additional safeguards to prevent identity  
104 theft, and I will soon introduce legislation designed to  
105 accomplish this goal. My legislation will be crafted around  
106 3 guiding principles. First, companies and entities that  
107 hold personal information must establish and maintain  
108 security policies to prevent the unauthorized acquisition of  
109 that data. Second, information considered especially  
110 sensitive such as credit card numbers should have even more  
111 robust security safeguards in place. And finally, consumers  
112 should be promptly informed when their personal information  
113 has been jeopardized.

114 The time has come for Congress to take decisive action.  
115 We need a uniformed national standard for data security and  
116 data breach notification and we need it now. While I remain  
117 hopeful that law enforcement officials will quickly determine  
118 the extent of these latest cyber attacks, they serve as a  
119 reminder that all companies have a responsibility to protect  
120 personal information and to promptly notify consumers when

121 that information has been put at risk. And we have a  
122 responsibility as lawmakers to make certain that this  
123 happens.

124 [The prepared statement of Mrs. Bono Mack follows:]

125 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
126 Mrs. {Bono Mack.} And now I would like to recognize the  
127 vice chairman of the--oh, I am sorry--the ranking member Mr.  
128 Butterfield for his 5-minute opening statement.

129 Mr. {Butterfield.} Let me thank you, Chairman Bono  
130 Mack, for your indulgence. I have been in my office with 28  
131 constituents, one of whom was a World War II veteran and  
132 several Vietnam veterans and they wanted to take pictures and  
133 you know that drill. And so I had to accommodate them as  
134 best I could. But we are here and thank you very much for  
135 convening this hearing today. And I certainly thank the two  
136 witnesses for your presence.

137 Madam Chairman, thank you for holding this hearing on  
138 data security and the recent breaches that we have seen at  
139 Sony and Epsilon. Last month, well over 100 million consumer  
140 records have been compromised as a result of those breaches,  
141 including full names, email and mailing addresses, the  
142 passwords, and maybe even credit card numbers. Those two  
143 major breaches illustrate that no company is safe from attack  
144 and that we must always operate at a heightened level of  
145 security and vigilance. No company wants its data  
146 compromised, and Sony and Epsilon are certainly no exception.

147 Sony was victim to hackers who stole nearly 100 million  
148 consumer records, and it took engineers several days to

149 realize that there was an intrusion. During that time,  
150 hackers had full access to Sony's servers. The breach that  
151 occurred at Epsilon was very large and involved the names and  
152 email addresses of about 50 of Epsilon's clients with  
153 conservative estimates of 60 million records stolen.  
154 Luckily, no critically sensitive information was stolen, but  
155 it easily could have.

156       It is important that businesses do all they can do to  
157 protect consumers from having their information fall into the  
158 wrong hands. For many Americans, shopping, paying bills, and  
159 refilling prescriptions and communicating with friends and  
160 family and even playing games are all done online. As people  
161 share more and more information online, the potential for  
162 personally identifiable information to be compromised  
163 increases exponentially. Names, physical addresses, dates of  
164 birth, Social Security numbers, and credit card numbers are  
165 just a few of the types of information that hackers are able  
166 to access and exploit.

167       While 46 States have laws requiring consumer  
168 notification when a breach occurs, there is currently no  
169 federal standard to address this. Moreover, there is no  
170 federal law requiring companies that hold PII to have  
171 reasonable safeguards in place to protect this information.  
172 Without a federal standard, I am concerned that American

173 consumers remain largely exposed online. And during the  
174 109th Congress and subsequent Congresses, members of this  
175 committee worked in a bipartisan fashion to develop the Data,  
176 Accountability, and Trust Act to address the issue of data  
177 security.

178         The DATA bill of the 111th Congress by my friend and  
179 former chairman of the subcommittee Mr. Rush from Illinois  
180 would have required entities holding data containing personal  
181 information to adopt reasonable and appropriate security  
182 measures to safeguard it and, in the event of a breach, to  
183 notify affected individuals. The DATA bill passed the House  
184 and the 111th Congress but our friends in the Senate did not  
185 act. The DATA bill is a good foundation to improve the  
186 security of e-commerce, something that is good for consumers  
187 and good for business. It would give American consumers more  
188 peace of mind about online transactions and make them more  
189 likely to continue and expand their use of online services.

190         And so, Madam Chairman, we have learned a lot from the  
191 breaches at Sony and Epsilon and I expect to learn more today  
192 from our two witnesses. I want you to know that I stand  
193 ready to work with you and our colleagues to pass a strong  
194 bipartisan data security bill like the DATA bill that we saw  
195 in the last session. I thank today's witnesses for their  
196 testimony and look forward to each of you. Thank you very

197 much. I yield back.

198 [The prepared statement of Mr. Butterfield follows:]

199 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
200 Mrs. {Bono Mack.} I thank the gentleman. Chairman  
201 Upton yielded his 5 minutes for an opening statement to me in  
202 accordance with committee rules. And as his designee, I now  
203 recognize Ms. Blackburn for 2 minutes.

204 Mrs. {Blackburn.} Thank you, Madam Chairman. I will  
205 submit my full statement.

206 A couple of comments. I think that the Sony and the  
207 Epsilon breaches raise a lot of questions with our  
208 constituents. What they are asking us is, number one, how do  
209 you minimize identity theft? Number two, they want proper  
210 notifications from the vendors that they are doing business  
211 with. And number three, they want to see better coordination  
212 with law enforcement. They feel as if this is missing. And  
213 I know that as we address this, what we are going to have to  
214 look at is better government coordination, incentives for  
215 industry cooperation in this issue, stricter penalty  
216 deterrents against hackers, and a flexible framework for risk  
217 assessment and breach alerts.

218 As we do this, I hope that we will continue to look at  
219 the threat of digital protection of intellectual property.  
220 The two are interrelated and they both deserve attention.  
221 And I have to tell you, with the new music cloud services  
222 from Apple, Google, and Amazon, my concern is there that we

223 hold everybody accountable and secure the integrity of that  
224 system.

225 I do want to highlight that on the issue of the illegal  
226 downloads and file sharing, my home State of Tennessee has  
227 just passed and signed into law a bill that puts in place  
228 penalties for this. They have made this a crime in our  
229 State, and I am glad they did it because losing content to  
230 the rogue websites not only becomes an issue for the  
231 entertainment industry, but it exposes consumers to viruses,  
232 dangerous products, and increases the likelihood of data  
233 theft.

234 So I thank you all for being here and I yield back my  
235 time.

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

237 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
238 Mrs. {Bono Mack.} I thank the gentlelady. And the  
239 chair recognizes Mr. Stearns for 2 minutes.

240 Mr. {Stearns.} Thank you, Madam Chair.

241 You know, I think it is mentioned by the chairwoman, the  
242 FTC recently reported 9 million Americans have fallen victim  
243 to identity theft. And I think it is sort of puzzling, a  
244 corporation as strong and comprehensive as Sony, they would,  
245 you would think, have the ability to certify that their data  
246 is secure. As recently mentioned, over 45 States have  
247 adopted a data breach notification requirement, but, of  
248 course, there is no law on a federal basis. So it is good  
249 that you folks are here so we can ask you some questions  
250 about, you know, perhaps if you know who the people were,  
251 what was the requirements that you set up in a corporation as  
252 extensive as Sony, and do you think there is a criminal case  
253 here that should be prosecuted? So there are lots of  
254 questions so I appreciate your coming here.

255 As many of you know, I had a bill when I was chairman of  
256 the subcommittee that we got out of the House.  
257 Unfortunately, it did not get through the Senate. And I have  
258 introduced it with Mr. Matheson again, which simply required  
259 the Federal Trade Commission to develop these regulations  
260 requiring persons that own or possess electronic data to

261 establish necessary security policies and procedures, as well  
262 as notification mechanism.

263         So both of our witnesses today certainly have within  
264 their power to provide the software, the data security  
265 provisions that are necessary. I think it must be puzzling  
266 to them as well as to us why this happened to them  
267 considering how sophisticated both of them are. I have had  
268 the opportunity to talk to them in my office, so it is very  
269 appreciative that you took the time to come here and talk to  
270 us and we look forward to your testimony. Thank you.

271         [The prepared statement of Mr. Stearns follows:]

272 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
273           Mrs. {Bono Mack.} I thank the gentleman. And the chair  
274 recognizes Mr. Olson for 1 minute.

275           Mr. {Olson.} I thank the chairwoman for her leadership  
276 in calling this timely hearing.

277           As we all learned this morning, overseas hackers from  
278 China hacked into Google email accounts. Like Sony, Epsilon,  
279 and now Google, my home State of Texas has experienced a  
280 massive data breach in April of this year when almost 3.5  
281 million Texans had their personal information, their names,  
282 mailing addresses, and Social Security numbers compromised  
283 from the office of the Texas Comptroller of Public Accounts,  
284 and it was posted to a public server.

285           There is a clear need for government, businesses, and  
286 citizens to work together to protect citizens' personal  
287 information. I look forward to working with the chairwoman  
288 on comprehensive data security legislation.

289           I thank the witnesses for coming. I yield back the  
290 balance of my time.

291           [The prepared statement of Mr. Olson follows:]

292           \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|

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

294 \*\*\*\*\* INSERT 3 \*\*\*\*\*

|  
295           Mrs. {Bono Mack.} I thank the gentleman and turn our  
296 attention to the panel. We have a single panel of very  
297 distinguished witnesses joining us today. Welcome. Each of  
298 you have a prepared statement that will be placed into the  
299 record, but if you could summarize your statements in your  
300 remarks, we would appreciate it.

301           On our panel, we have Jeanette Fitzgerald, General  
302 Counsel for Epsilon Data Management, LLC. Also testifying is  
303 Tim Schaaff, President, Sony Network Entertainment  
304 International. Good afternoon, and thank you both very much  
305 for coming. You will each be recognized, as I said, for 5  
306 minutes. To help you keep track of time, there is a clever  
307 little device in front of you: red, yellow, green. And when  
308 the light turns yellow, please summarize as you would a  
309 traffic light.

310           So Ms. Fitzgerald, you are recognized for 5 minutes.  
311 And please remember the microphone and pull it close to your  
312 mouth if you would.

|  
313 ^STATEMENTS OF JEANETTE FITZGERALD, GENERAL COUNSEL, EPSILON  
314 DATA MANAGEMENT, LLC; AND TIM SCHAAFF, PRESIDENT, SONY  
315 NETWORK ENTERTAINMENT INTERNATIONAL

|  
316 ^STATEMENT OF JEANETTE FITZGERALD

317 } Ms. {Fitzgerald.} --Ranking Member Butterfield, and  
318 distinguished members of--

319 Mrs. {Bono Mack.} Sorry. Excuse me. Would you pull  
320 the microphone up?

321 Ms. {Fitzgerald.} Closer? Better?

322 Mrs. {Bono Mack.} Thank you.

323 Ms. {Fitzgerald.} Good morning. Chairman Bono Mack,  
324 Ranking Member Butterfield, and distinguished members of the  
325 subcommittee, my name is Jeanette Fitzgerald, and I am the  
326 general counsel for Epsilon Data Management. Thank you for  
327 inviting me to present Epsilon's testimony on data security.  
328 I hope that I can provide information today in going forward  
329 that will act as a helpful resource as you consider data  
330 security legislation that is in the best interest of both  
331 consumers and business. My full written testimony has been  
332 submitted for the record. I will summarize it here and hope  
333 to leave you with three main points.

334 First, who is Epsilon and how do we provide important  
335 data management services for our clients? Second, how the  
336 attack of March 30 occurred and what we are doing to  
337 apprehend the perpetrators and improve our own data security.  
338 And finally, why we think national data breach notification  
339 legislation is important.

340 Epsilon is the leading provider of permission-based  
341 email marketing services. Our clients, some of the world's  
342 largest and best-known consumer and financial services brands  
343 count on us to send their email messages to their customers,  
344 the individual consumer. And as we all know, major brands  
345 use email messages to provide consumers with timely  
346 information about new products and sales and events, among  
347 other things. Epsilon ensures that these email messages  
348 comply with applicable legal requirements, including CAN-SPAM  
349 Act.

350 To earn and keep our clients' trust, Epsilon became the  
351 first in the industry in 2006 to certify that its information  
352 security program complied with the standards issued by the  
353 International Association of Standardization, known as ISO.  
354 ISO, a highly regarded organization, is recognized by over  
355 160 countries around the world, including the United States,  
356 as identifying best practices for information security  
357 management. The standards are demanding, requiring over a

358 year to earn initial certification. We are proud that  
359 Epsilon leads the industry and that we have achieved yearly  
360 recertification, which requires proof that the company is  
361 improving its security program each year.

362 Notwithstanding our internal security procedures and our  
363 compliance with these rigorous data security standards, as  
364 you know, Epsilon was the victim of a criminal hacking  
365 incident at the end of March. Since our information security  
366 program was designed to identify and respond to attacks and  
367 threats, we were quickly able to detect the unauthorized  
368 download activity, which triggered Epsilon's security  
369 incident response program.

370 Our investigation, both internal and with an independent  
371 third party, is coordinated closely with the Secret Service  
372 and is still ongoing. But we can say that the initial  
373 investigation confirms that only email addresses and, in some  
374 cases, first and last names were affected by this attack.  
375 Again, only email addresses and, in some cases, first and  
376 last names were affected. The details of what happened after  
377 the attack are in my written statement that has been  
378 submitted for the record. We are greatly troubled that this  
379 criminal incident has called into question our commitment to  
380 data security. But I want to leave you with four main points  
381 about what happened and how Epsilon responded.

382 First, our internal response to the criminal attack was  
383 immediate. We isolated computers and changed employee access  
384 rights. Second, our forensics investigation began within  
385 hours. We also reached out to law enforcement just as  
386 quickly. Third, notification to our clients also occurred on  
387 the same day, and we released a public statement and posted  
388 additional public information on our website shortly  
389 thereafter. And finally, now and going forward, we reiterate  
390 our commitment to working with the Secret Service,  
391 apprehending the hackers, and improving our own security.

392 Companies like Epsilon are on the frontlines in the  
393 fight against data theft. We also believe Congress has an  
394 important role to play in protecting consumers. To that end,  
395 Epsilon fully supports legislation that would create a  
396 uniform standard for data breach notification. The current  
397 patchwork of over 45 individual State breach notification  
398 laws is confusing. A uniform national law, on the other  
399 hand, would provide predictability and equitable protection  
400 for consumers, regardless of their State of residence.

401 Chairman Bono Mack, Ranking Member Butterfield, and  
402 members of the subcommittee, we look forward to working with  
403 you as the legislative process moves forward. I sincerely  
404 hope that the information I am able to provide at this  
405 hearing is helpful to the subcommittee as it considers this

406 critical issue. Thank you.

407 [The prepared statement of Ms. Fitzgerald follows:]

408 \*\*\*\*\* INSERT 1 \*\*\*\*\*

|  
409           Mrs. {Bono Mack.} Thank you, Ms. Fitzgerald. And Mr.  
410 Schaaff, you are recognized for 5 minutes.

|  
411 ^STATEMENT OF TIM SCHAAFF

412 } Mr. {Schaaff.} Thank you. Chairman Bono Mack, Ranking  
413 Member Butterfield, and other distinguished members of the  
414 subcommittee, thank you for providing Sony with this  
415 opportunity to testify on cyber crime and data security.

416 My name is Tim Schaaff and I am president of Sony  
417 Network Entertainment International, a subsidiary of Sony  
418 Corporation based in California, where we employ  
419 approximately 700 people in five offices around the State. I  
420 am chiefly responsible for the business and technical aspects  
421 of Sony's PlayStation Network and Curiosity, an online  
422 service that allows consumers to access movies, television  
423 shows, music and video games. Sony Network Entertainment,  
424 Sony Online Entertainment--another subsidiary of Sony's--and  
425 millions of our customers were recently the victims of an  
426 increasingly common digital age crime--a cyber attack.  
427 Indeed, we have been reminded in recent days of the fact that  
428 no one is immune from the threat of cyber attack.  
429 Businesses, government entities, public institutions, and  
430 individuals can all become victims.

431 The attack on us, we believe, unprecedented in its size  
432 and scope. Initially anonymous, the underground group

433 associated with last year's WikiLeaks-related cyber attacks  
434 openly called for and carried out massive denial-of-service  
435 attacks against numerous Sony internet sites in retaliation  
436 for Sony bringing action in Federal Court to protect its  
437 intellectual property. During or shortly after those  
438 attacks, one or more highly skilled hackers infiltrated the  
439 servers of the PlayStation Network and Sony Online  
440 Entertainment.

441 Sony Network Entertainment and Sony Online Entertainment  
442 have always made a concerted and substantial effort to  
443 maintain and improve their data security systems. We hired a  
444 well respected and experienced cyber security firm to enhance  
445 our defenses against the denial-of-service attacks threatened  
446 by anonymous, but unfortunately, no entity can foresee every  
447 potential cyber security threat.

448 We have detailed for the subcommittee in our written  
449 testimony the timeline from when we first discovered the  
450 breach. But to briefly summarize, the first indication of a  
451 breach occurred on Tuesday, April 19 of this year. On  
452 Wednesday, April 20, we mobilized an investigation and  
453 immediately shut down all of the PlayStation Network services  
454 in order to prevent additional unauthorized activity. After  
455 two highly respected technical forensic firms were retained  
456 to assist in a time-consuming and complicated investigation,

457 on Friday, April 22, we notified PlayStation Network  
458 customers via post on the PlayStation blog that an intrusion  
459 had occurred. After a third forensic firm was retained, on  
460 Monday, April 25, we were able to confirm the scope of the  
461 personal data that we believed had been accessed. And  
462 although there was no evidence credit card information had  
463 been accessed, we could not rule out the possibility.

464         Therefore, the very next day, Tuesday, April 26, we  
465 issued a public notice that we believed the personal  
466 information of our customers had been taken. And that while  
467 there was no evidence that credit card data was taken, since  
468 we could not rule out the possibility, we had to acknowledge  
469 that it was possible. We also posted this on our blog and  
470 began to email each of our accountholders directly. We did  
471 not merely make statements on our blog.

472         On Sunday, May 1, Sony Online Entertainment, a multi-  
473 player online videogame network, also discovered that data  
474 may have been taken. On Monday, May 2, just one day later,  
475 Sony Online Entertainment shut down this service and notified  
476 customers directly that their personal information may have  
477 also been compromised. Throughout this time, we felt a keen  
478 sense of responsibility to our customers. We shut down the  
479 networks to protect against further unauthorized activity.  
480 We notified our customers promptly when we had specific,

481 accurate, and useful information. We thanked our customers  
482 for their patience and loyalty and addressed their concerns  
483 arising from this breach with identify theft protection  
484 programs for the U.S. and other customers around the world  
485 where available, as well as a welcome-back package of  
486 extended and free subscriptions, games, and other services.  
487 And we worked to restore our networks to stronger security to  
488 protect our customer's interests.

489         Let me address the specific issues you are considering  
490 today: notification of consumers when data breaches occur.  
491 Laws and common sense provide for companies to investigate  
492 breaches, gather the facts, and then report data losses  
493 publicly. If you reverse that order issuing vague or  
494 speculative statements before you have specific and reliable  
495 information, you either send false alarms or so many alarms  
496 that these warnings may be ignored. We therefore support  
497 federal data breach legislation and look forward to working  
498 with the subcommittee on the particulars of the bill.

499         One final point--as frustrating as the loss of networks  
500 for playing games was for our customers, the consequences of  
501 cyber attacks against financial or defense institutions can  
502 be devastating for our economy and security. Consider the  
503 fact that defense contractor Lockheed Martin and the Oakridge  
504 National Laboratory, which helps the Department of Energy

505 secure the Nation's electric grid, were also cyber attacked  
506 within the past 2 months.

507         By working together to enact meaningful cyber security  
508 legislation, we can limit the threat posed to us all. We  
509 look forward to this initiative to make sure that consumers  
510 are empowered with the information and tools they need to  
511 protect themselves from cyber criminals. Thank you very  
512 much.

513         [The prepared statement of Mr. Schaaff follows:]

514 \*\*\*\*\* INSERT 2 \*\*\*\*\*

|  
515           Mrs. {Bono Mack.} Thank you, Mr. Schaaff. And I would  
516 like to thank both of you for your opening statements, as  
517 well as for your unique insight into these disturbing data  
518 breaches. I am confident that the lessons learned with  
519 assist us in our efforts to develop new online safeguards for  
520 American consumers.

521           And I am going to recognize myself for the first 5  
522 minutes of questioning.

523           And, Mr. Schaaff, given the extreme makeover of Sony's  
524 online security protocols, it does beg the question why  
525 weren't many of these safeguards, such as having a chief  
526 security information officer in place before the April data  
527 breaches?

528           Mr. {Schaaff.} We believe that the security that we had  
529 in place was very, very strong and we felt that we were in  
530 good shape. However, as the attacks indicated, the intensity  
531 and sophistication of the hack was such that even despite  
532 those best measures that we had taken, it was not sufficient.  
533 And as we recognize moving forward that the scrutiny that we  
534 are likely to be under from the hackers will continue, we  
535 have made additional commitments to enhance the security of  
536 our networks.

537           In addition, we had been working for some months now,

538 more than 18 months to expand both the capacity and security  
539 of our network. We are a new business but we are a very  
540 fast-growing business.

541 Mrs. {Bono Mack.} All right. Let me jump ahead.

542 Mr. {Schaaff.} Sure.

543 Mrs. {Bono Mack.} You indicated with Sony in the May 3  
544 letter that you contacted the FBI on April 22, which was 2  
545 days after it determined the breach had in fact occurred.  
546 Why did Sony wait 2 days to notify law enforcement?

547 Mr. {Schaaff.} My understanding is that we notified  
548 them as soon as we had something clear that we could report  
549 that indicated some sign of external intrusion that would be  
550 unauthorized or illegal.

551 Mrs. {Bono Mack.} Your testimony indicates four servers  
552 were taken offline on April 19 before you pulled the plug on  
553 all 130 servers. Can you tell us what information was  
554 different that was stored on those initial four servers?

555 Mr. {Schaaff.} Well, these were part of a larger  
556 network of machines and we believed this was just the first  
557 entry point that the hacker may have used to get into the  
558 network, and upon discovering them, we immediately shut them  
559 down. But there were other servers that were also attacked  
560 by the hackers as well.

561 Mrs. {Bono Mack.} Some media reports indicate Sony's

562 servers may not have had up-to-date patches or firewalls  
563 prior to the attack. Is that true?

564 Mr. {Schaaff.} That is actually patently false. The  
565 Apache servers were fully up to date, fully patched. And in  
566 fact, we had had several layers of firewalls in place, also  
567 contrary to so many of the things you may have read on the  
568 internet. As you know, the internet is not always a reliable  
569 source of factual information.

570 Mrs. {Bono Mack.} And you state that you believe the  
571 cyber attack on Sony was unprecedented in both size and  
572 scope. Can you explain why you believe it is unprecedented?

573 Mr. {Schaaff.} Well, we believe that the sophistication  
574 of the attack, the collection of activities that were  
575 undertaken, the period of time in which the hackers were  
576 carefully exploring the network, and then ultimately the  
577 scope of the service that was breached makes it quite a  
578 remarkable attack. And despite the deep security measures  
579 that we had taken, it was nevertheless insufficient to guard  
580 against these attacks.

581 Mrs. {Bono Mack.} Was the consumer data you held  
582 encrypted? And why or why not?

583 Mr. {Schaaff.} So, of course, the credit card  
584 information that was held was encrypted. Password login data  
585 was protected using cryptographic hash functions. And these

586 practices are in line with industry practice.

587           Mrs. {Bono Mack.} Thank you. Ms. Fitzgerald, would  
588 greater security requirements have prevented your breach?  
589 And if not, what added protection are your new security  
590 measures providing?

591           Ms. {Fitzgerald.} At the time, we had very extensive  
592 security as I noted in my opening statement and the written  
593 statement I provided. We have continued through the  
594 investigation to evaluate additional things that may be done  
595 to strengthen both our networks and any of the access points.  
596 We have also decided to hire some outside experts to even  
597 evaluate the network further and see if there is anything  
598 else in different parts of our network that need to be  
599 adjusted.

600           Mrs. {Bono Mack.} Coming as a consumer who received  
601 multiple notices about your breach, there are also  
602 indications that consumers received notice of the breach from  
603 your business customers for which, in some cases, they hadn't  
604 had a purchase or customer relationship for 4 or 5 years. Do  
605 you ever purge your data and why do you hold onto information  
606 for as long as you do?

607           Ms. {Fitzgerald.} So let me step back a second to  
608 remind everyone how Epsilon plays in this. Epsilon is a  
609 service provider to the well-known names that you may have

610 received notifications from, and they have the relationship  
611 with the consumer. What data we hold is determined by the  
612 client, and the client then tells us what to hold and what we  
613 then do with it in terms of sending out notices or any sort  
614 of marketing messages is entirely up to the client. It is  
615 not--

616 Mrs. {Bono Mack.} Do you advise them on when it might  
617 be a good time to purge data?

618 Ms. {Fitzgerald.} It depends on what they want to do  
619 with the data. And there is also opt-out data that would  
620 have been held because in order to comply with CAN-SPAM, you  
621 have to maintain records of who has opted out. So if, 2  
622 years ago, you opted out and you haven't had any activity,  
623 that list would still be there because you have to comply  
624 with CAN-SPAM. So we have to be able to duplicate or de-  
625 duplicate and take those names out any time that we do a  
626 mailing.

627 Mrs. {Bono Mack.} Okay. Thank you. My time has  
628 expired. I will recognize the ranking member, Mr.  
629 Butterfield, for his 5 minutes.

630 Mr. {Butterfield.} Thank you, Madam Chairman.

631 Mr. Schaaff, let me start with you and if I have any  
632 time remaining, I will go over to Ms. Fitzgerald.

633 Mr. Schaaff, I understand that your internal

634 investigation has not turned up any evidence suggesting that  
635 credit card data was taken from the network, but to me, that  
636 doesn't necessarily mean that the data was not taken, just  
637 that you haven't turned up any digital fingerprints that  
638 would allow you to know with certainty that it was taken.  
639 And I think you see what I am saying there. Help me with  
640 that. How certain are you that the data was not taken in the  
641 attack?

642         Mr. {Schaaff.} Well, as you know, we have been engulfed  
643 in an intensive investigation over the past 6 weeks since the  
644 breach occurred, and we have looked deeply at the logs  
645 related to the databases. And in those logs we have found no  
646 clear evidence that there was any access made to the credit  
647 card information, and we found plenty of evidence that  
648 suggests that that data was not accessed. That is the basis  
649 for today's statements that we do not believe the credit card  
650 information was compromised.

651         Mr. {Butterfield.} Now, in your testimony, you  
652 mentioned that the attack took place on April 19, that the  
653 PlayStations were shut down on April 20, and that you did  
654 something on April 22. Help me with that if you could shed  
655 some light on what you did on April 22.

656         Mr. {Schaaff.} On April 22, this was the point at which  
657 we first notified consumers that there had been an intrusion.

658 We were trying to understand what had happened to the  
659 network, and we were actively beginning the investigation of  
660 that breach. And at the point that we were able to determine  
661 that there had been an intrusion, we immediately notified  
662 consumers so that they would be aware of what had occurred,  
663 even though at that time we were not yet able to confirm  
664 precisely which data may have been compromised.

665 Mr. {Butterfield.} So is it your testimony that on  
666 April 22, you began the process of notifying the consumers?

667 Mr. {Schaaff.} Well, we notified them on the  
668 PlayStation blog of the intrusion, but then on April 26, we  
669 followed that up with an additional notification regarding  
670 more specifics related to the actual data that may have been  
671 breached and we began immediately notifying consumers  
672 starting from that date via email of the breach as well.

673 Mr. {Butterfield.} But the April 22 announcement was  
674 simply on the internet? It was on the blog?

675 Mr. {Schaaff.} That was posted on the PlayStation blog.  
676 The PlayStation blog is one of the most active and popular  
677 blogs on the web. It is currently ranked about number 20,  
678 just behind the White House blog. So it is a very, very  
679 expected place for our consumers to look for information.

680 Mr. {Butterfield.} Do you have any way of knowing how  
681 many consumers actually read the statement?

682 Mr. {Schaaff.} I don't know the answer to that off the  
683 top of my head. We can investigate and--

684 Mr. {Butterfield.} But 7 days after the breach was when  
685 official notification was issued?

686 Mr. {Schaaff.} We were not able to determine until the  
687 day that we had notified consumers. We were searching for  
688 evidence that would allow us to confirm the status of the  
689 credit card information and not being able--

690 Mr. {Butterfield.} Do you think 7 days was a reasonable  
691 time?

692 Mr. {Schaaff.} Actually, what has been interesting from  
693 my perspective is that we have continued this investigation  
694 in the successive weeks, and as you hear me speaking today,  
695 some of our conclusions with respect to credit card  
696 information have changed somewhat from our original  
697 statements. And that change has occurred because of the  
698 continuing investigation. In the abundance of caution, we  
699 acknowledge the possibility that credit cards would have been  
700 taken in our announcements on the 26th. But as you can see,  
701 the situation changes as the investigation proceeds, and we  
702 felt it would have been irresponsible if we had notified  
703 consumers earlier with partial or incomplete information.

704 Mr. {Butterfield.} But you have, based on your  
705 experience here, made some corrections and some adjustments

706 in the credit card data that you collect?

707 Mr. {Schaaff.} We have been working to increase the  
708 security of the entire network and additional controls  
709 related to credit card data have also been put in place, yes.

710 Mr. {Butterfield.} And how do these measures compare to  
711 those for the other types of personal information that you  
712 have, the credit card data versus the other information?

713 Mr. {Schaaff.} Yes, excuse me. The credit card  
714 information is the most highly protected and guarded  
715 information. It is all encrypted and so even if it is taken,  
716 it is not likely to be useful to the hacker.

717 Mr. {Butterfield.} Is it true that user passwords were  
718 hashed and not encrypted? Is that true?

719 Mr. {Schaaff.} That is true. It is true that they were  
720 hashed using cryptographic hash functions. That is an  
721 industry practice which is very standard. It is not an  
722 unusual practice at all.

723 Mr. {Butterfield.} Industry standard. Well, why don't  
724 you use any type of encryption in your procedures?

725 Mr. {Schaaff.} It is a form of protection that is very,  
726 very closely related to encryption, and I am not an expert in  
727 cryptography so I am not sure that I could answer the  
728 question in a more detailed way.

729 Mr. {Butterfield.} What is irreversible encryption?

730 Mr. {Schaaff.} Irreversible encryption is my  
731 understanding of the definition of a cryptographic hash. I  
732 am sorry. This is--wait. Okay.

733 Mr. {Butterfield.} Ms. Fitzgerald, your testimony  
734 states that Epsilon's internal investigation revealed that  
735 the login credentials of the employee who reported unusual  
736 and suspicious download activity had been compromised. And  
737 in layman's terms, I suppose, I assume this means that the  
738 employees credentials had been hijacked and been used by a  
739 hacker to carry out the intrusion into your network and to  
740 steal consumers' email addresses. Can you please tell me a  
741 little bit more about what that means, that the employee's  
742 login credentials were compromised?

743 Ms. {Fitzgerald.} Well, what we had understood during  
744 the investigation is that the credentials were somehow used  
745 based on the logs, though not necessarily by that person, to  
746 actually download that information. That is why we then  
747 immediately--our system kicked into place and immediately we  
748 saw that there was improper downloads and so our security  
749 system kicked in and then we knew that there was a problem  
750 and we shut their access down and anybody else who had  
751 credentials at that level and took that computer off the  
752 system.

753 Mr. {Butterfield.} Thank you. My time has expired.

754 Mrs. {Bono Mack.} I thank the gentleman and recognize  
755 the gentleman from Florida, Mr. Stearns, for 5 minutes.

756 Mr. {Stearns.} Thank you, Madam Chair. Let me be sure  
757 I understand, Ms. Fitzgerald, exactly what was taken. It is  
758 our understanding emails were taken and the name of the  
759 people whose email was taken. Is that correct?

760 Ms. {Fitzgerald.} I am sorry. Was that to me?

761 Mr. {Stearns.} Yes.

762 Ms. {Fitzgerald.} I am sorry.

763 Mr. {Stearns.} What was actually taken, as I understand  
764 it, is emails--

765 Ms. {Fitzgerald.} It was email addresses, and in some  
766 cases, first and last names.

767 Mr. {Stearns.} First and last names. Okay. And that  
768 was all?

769 Ms. {Fitzgerald.} Yes.

770 Mr. {Stearns.} And you said that you notified all 50 to  
771 75 customers. Is that correct?

772 Ms. {Fitzgerald.} There were about 50 customers of our  
773 clients, that were affected.

774 Mr. {Stearns.} Okay.

775 Ms. {Fitzgerald.} And we notified them.

776 Mr. {Stearns.} Would you provide the committee the  
777 complete list of those?

778 Ms. {Fitzgerald.} The names of those clients are  
779 subject to agreements that we have with them, and we are  
780 supposed to keep those confidential.

781 Mr. {Stearns.} So you cannot provide us--

782 Ms. {Fitzgerald.} So we notified them promptly so they  
783 could--

784 Mr. {Stearns.} No, I know you notified them, but you  
785 cannot provide the committee with these names? Is that what  
786 you are saying today?

787 Ms. {Fitzgerald.} Not at this point, no.

788 Mr. {Stearns.} Now, I have in our material that some of  
789 these people are J.P. Morgan Chase, Capital One, Citibank,  
790 Best Buy, Verizon, Target, Home Shopping Network, and  
791 Verizon. Is that part of the 50 to 75?

792 Ms. {Fitzgerald.} I recognize most of those names as  
793 being ones that sent us notification--

794 Mr. {Stearns.} They are people that have huge number of  
795 people, so the impact of this 50 to 75, we cannot even  
796 comprehend how many Verizon has. So can you extrapolate, not  
797 telling us in detail, but if Verizon is one of your customers  
798 and you had a breach with the emails and names, does that  
799 mean that perhaps millions of names from Verizon had been  
800 breached?

801 Ms. {Fitzgerald.} There could be many.

802 Mr. {Stearns.} Just yes or no.

803 Ms. {Fitzgerald.} Yes.

804 Mr. {Stearns.} Yes, okay. Now, with Sony, the question  
805 is, as I understand it, the password for the Sony PlayStation  
806 was breached. Is that correct?

807 Mr. {Schaaff.} Well, we believe that there were a  
808 number of different types of information accessed, including  
809 first name and last name, address, date of birth, login,  
810 password, login address--

811 Mr. {Stearns.} For the Sony PlayStation?

812 Mr. {Schaaff.} For the Sony PlayStation Network, yes.

813 Mr. {Stearns.} Okay. And what about their credit  
814 cards?

815 Mr. {Schaaff.} As I said, we had originally stated that  
816 there was a possibility. We could not rule out the  
817 possibility that the credit card information had been  
818 accessed. At this point in time, we do not see any evidence  
819 that it has been.

820 Mr. {Stearns.} Okay. When you look at the person's  
821 credit card together with personal information, his password  
822 for Sony PlayStation, would one person have all of that  
823 breached for that one person or is it segmented so somebody  
824 got their password, somebody got their credit card, somebody  
825 got their person or is all this information together when it

826 was breached?

827           Mr. {Schaaff.} It is difficult for us to know exactly  
828 which data was taken, but it is likely that they would have  
829 been taken together, but we don't know for which accounts  
830 that would have been.

831           Mr. {Stearns.} And what is a conservative estimate the  
832 number of people were affected by this breach?

833           Mr. {Schaaff.} Well, so we have announced that there  
834 were approximately 77 million accounts that could have been  
835 accessed. When we took the network offline, obviously all of  
836 our customers were affected for the period of time that the  
837 network has been down, but that is part of the reason why we  
838 have provided the identity theft insurance, identity theft  
839 protection program, and these welcome back programs was to  
840 appreciate and acknowledge the loss of access to the network  
841 that our customers experienced and to address the concerns  
842 that they may have regarding the loss of their personal  
843 information.

844           Mr. {Stearns.} Is it true that you brought suit to  
845 protect your IP against the hackers of PlayStation III  
846 device?

847           Mr. {Schaaff.} That is true.

848           Mr. {Stearns.} Why did you bring this suit?

849           Mr. {Schaaff.} Well, just like the music industry and

850 the movie industry, the PlayStation business is built upon  
851 intellectual property. Content providers invest millions of  
852 dollars to create titles that we then help them to distribute  
853 in our business and the employment of literally tens of  
854 thousands of people around the country.

855 Mr. {Stearns.} Knowing what has happened to you with  
856 this breach, would you say that you would do it again?

857 Mr. {Schaaff.} I am sorry. I didn't hear the question.

858 Mr. {Stearns.} Knowing what has happened with this  
859 breach, would you go ahead and have done that suit again in  
860 hindsight?

861 Mr. {Schaaff.} Well, I think this is one of the great  
862 challenges right now is how do companies protect their  
863 content businesses? I mean I think we made the right  
864 decision. Did it have consequences? It appears to have had  
865 some fairly negative consequences for the company. But if we  
866 hadn't done something, I think it would be playing out in a  
867 different company later on.

868 Mr. {Stearns.} Okay.

869 Mr. {Schaaff.} I think this is a big issue for the  
870 Nation.

871 Mr. {Stearns.} Now, assuming we have federal  
872 legislation, do you think federal legislation to address  
873 security breaches would help? Because I understand both of

874 you are in States where we have state legislation and that  
875 didn't seem to necessarily force you to have a secure data  
876 security department. So why would federal legislation make  
877 it better than the States who have already passed? And you  
878 didn't comply, evidently, with the States.

879 Mr. {Schaaff.} Well, actually, I think that the issue  
880 regarding the States' rights--I am not a lawyer. Let me  
881 mention up front I am not a lawyer.

882 Mr. {Stearns.} Right.

883 Mr. {Schaaff.} But my understanding here is that there  
884 are a variety of laws in a number of the States, but the laws  
885 are often seemingly in conflict and they can create very  
886 complicated situations for us to understand how we should  
887 behave properly with regard to notification obligations.  
888 Regarding the security of the network, I think the evidence  
889 of Epsilon, of Sony, of many other companies that have been  
890 reported in the news in the last several weeks indicates that  
891 despite spending millions of dollars to secure your networks,  
892 despite all of the best methods known to us, our networks are  
893 not 100 percent protected. It is a process that requires  
894 continual investment, and we do that, but I think without  
895 additional support from the government, it is unlikely we  
896 will all collectively be successful, and that will threaten  
897 the livelihood of the internet, the growing internet economy.

898 Mr. {Stearns.} Thank you.

899 Mrs. {Bono Mack.} The gentleman's time has expired.

900 The chair recognizes Mr. Guthrie for 5 minutes.

901 Mr. {Guthrie.} Thank you, Madam Chairman, for having  
902 this hearing. I appreciate it very much.

903 So just to follow up on what Mr. Stearns said, the  
904 patchwork of state laws, the different state jurisdictions  
905 complicated your ability to respond? You didn't say that.  
906 Is that what I heard?

907 Mr. {Schaaff.} I was responding specifically to the  
908 issue about the notification obligation.

909 Mr. {Guthrie.} Right, the notification state laws.

910 Mr. {Schaaff.} It is my understanding that there are  
911 some conflicting obligations there.

912 Mr. {Guthrie.} So a federal standard would be--

913 Mr. {Schaaff.} A federal standard that would preempt  
914 the states would be extremely helpful.

915 Mr. {Guthrie.} Okay. I just want to get kind of the  
916 nature--so Epsilon is a vendor for you? Is Epsilon a vendor  
917 for Sony? So did the hacker go to Epsilon into Sony or Sony  
918 to Epsilon to get to the other--how did that work?

919 Mr. {Schaaff.} I am sorry. Let me clarify. These are  
920 actually two completely separate breach events.

921 Mr. {Guthrie.} Okay.

922 Mr. {Schaaff.} So the activity at Epsilon was  
923 completely unrelated to--as far as we know--what happened at  
924 Sony.

925 Mr. {Guthrie.} So you are not a vendor with Epsilon?  
926 This is two completely separate--okay. So the other  
927 customers--okay. I was thinking--I apologize. But your  
928 other customers, they came--the Epsilon, they got to your  
929 system, and then through your system were able to--at least  
930 the companies that you notified, the Verizons, the Krogers  
931 that was mentioned earlier, that was how that breach worked?

932 Ms. {Fitzgerald.} So as a vendor, our ability to send  
933 out email addresses on behalf of those clients requires us to  
934 maintain those email addresses for them.

935 Mr. {Guthrie.} Right.

936 Ms. {Fitzgerald.} And that is how the hackers got in  
937 and got that information.

938 Mr. {Guthrie.} Okay. Okay. Has Sony been victim  
939 before of any type of breach? And if so, how did that--not  
940 to this level, I know, but--

941 Mr. {Schaaff.} We certainly experience a constant level  
942 of fraud, and we are under regular probing by hackers and  
943 others. I mean I think it is a standard part of anybody who  
944 is in the internet business these days.

945 Mr. {Guthrie.} And for both of you, too, I know I am

946 manufacturing background and we did ISO 9000, which was a set  
947 of standards for quality control. They have ISO 14000, a set  
948 of standards for environmental--and they are good practices  
949 to follow, but they leave a lot of interpretation to the  
950 businesses because otherwise they are formed by committee,  
951 and it would be difficult to change every time something  
952 needs to be changed. I am not familiar with this particular  
953 standard that you are talking about, but is it sufficient if  
954 you follow the ISO standards to--I guess my question is your  
955 industry is so fast-changing that when you are in the  
956 automotive industry, which I am in, you put a standard in  
957 place, it takes a while for things to innovate that the  
958 standard is out of date. It appears to me when I saw ISO  
959 that it would be difficult for them to keep up with the  
960 changes in the industry or, I guess what I am saying, the  
961 ability of people who hack to innovate to find new ways into  
962 your system. So is it sufficient--I guess ISO being  
963 certified sufficient, you think?

964 Ms. {Fitzgerald.} We don't use the ISO as the only  
965 thing we do. We have lots of audits by our clients. We have  
966 70 audits we have to do. And then, frankly, we have our own  
967 security program where we are continually trying to upgrade  
968 our systems and to make sure that we make things as tight as  
969 we can, but the hackers are very sophisticated. This wasn't

970 some guy in a garage just coming after us. These are  
971 sophisticated guys. And I have talked to the Secret Service  
972 enough times now to know that we are not the only one and  
973 that they are working with the FBI. And there is a concerted  
974 effort to go after these guys.

975 Mr. {Schaaff.} Um-hum. Yeah, I would concur. I mean I  
976 think these guidelines and standards are important for the  
977 industry to move forward, but they are far from sufficient.  
978 And if they had been sufficient, I, you know, I wouldn't be  
979 here. And I think that we are all under attack and without  
980 additional measures to be taken and without kind of constant  
981 renewal of our practices, it is not going to be sufficient to  
982 fight the latest attacks.

983 Mr. {Guthrie.} Okay. Thank you. I guess one thing  
984 that I am really kind of concerned about as we move forward,  
985 I know Sony--any time you spend money because somebody did  
986 something illegal, that is an inefficiency to everybody. But  
987 the two- or three-store small business in Kentucky that  
988 maintains their clients files and just having the resources  
989 to be able to respond to protect their clients, to protect  
990 their customers. And just do you have any estimate of how  
991 much money just these events are going to cost your firm and  
992 hits, you know, the economy overall because that is what--

993 Mr. {Schaaff.} I believe we have made statements

994 publicly estimating a cost something in the range of \$170  
995 million for this particular incident. And obviously, as you  
996 note, for smaller businesses, number one, the ability to  
997 secure their networks as effectively is less because of the  
998 economics of that. And the evidence that I have seen in  
999 various reports suggest that the prevalence of successful  
1000 attacks on small and midsize businesses is even higher than  
1001 we see with the larger companies. It is a scary situation.

1002 Mr. {Guthrie.} Well, thank you. I yield back to the  
1003 chairwoman.

1004 Mrs. {Bono Mack.} I thank the gentleman and the chair  
1005 notes that we are being called to the floor for votes. My  
1006 intention is to try to get through two more member  
1007 questioning 5-minute segments before we recess. So the chair  
1008 now recognizes Mr. Olson for 5 minutes.

1009 Mr. {Olson.} I thank the chairwoman. And again, I  
1010 thank the witnesses for coming and giving us your expertise,  
1011 your time today.

1012 As I stated in my opening statement, my home State of  
1013 Texas experienced a serious and troubling data breach earlier  
1014 this year. Names, addresses, Social Security numbers, and in  
1015 some cases, birthdates and drivers' license numbers of state  
1016 retirees and unemployment beneficiaries were posted  
1017 unencrypted on a public server. In response, our state

1018 attorney general and the FBI have launched a criminal  
1019 investigation into this data breach. Unfortunately, these  
1020 kind of breaches are happening more frequently and they cause  
1021 businesses tens of billions of dollars annually. The Federal  
1022 Trade Commission estimates that 9 million individuals in the  
1023 United States have their identities stolen every year. This  
1024 is the equivalent of approximately 17 identities stolen every  
1025 minute. That means that during the course of this hearing,  
1026 if all of my colleagues and I take up our full 5 minutes, 85  
1027 IDs across this country will have been stolen.

1028 In response to the Texas data breach, the comptroller of  
1029 public accounts launched a website called Texas Safeguard,  
1030 which was created as a tool for Texans to receive up-to-date  
1031 information about the breach, along with recommended security  
1032 steps to take. And of note, they actually put a toll-free  
1033 number up for folks to call and the comptroller is offering  
1034 credit monitoring at no charge. There is also a frequently-  
1035 asked-questions page which outlines six steps people can take  
1036 to protect themselves.

1037 But this burden is placed upon these victims of this  
1038 breach and they have got to spend their own time enrolling in  
1039 credit monitoring, placing fraud alerts on their credit  
1040 files, requesting credit reports, and so on, and so on, and  
1041 so on. Ms. Fitzgerald, Mr. Schaaff, given the breaches your

1042 companies have experienced and all the heartache and lost  
1043 revenue, all the upset customers, all the resources you have  
1044 had to expend to determine how these breaches occurred, I  
1045 don't want to put words in your mouth, but you do think that  
1046 there is a clear need for a comprehensive federal data breach  
1047 and notification law, one that will create a uniform standard  
1048 and preempt the current patchwork of state laws? Yea, nay?

1049 Ms. {Fitzgerald.} I do believe that it would be great  
1050 if we had a federal data breach notification law that did  
1051 preempt all of the state laws so it would be straightforward  
1052 and companies would know exactly what they needed to take  
1053 care of and who they needed to notify and when they needed to  
1054 notify?

1055 Mr. {Olson.} Mr. Schaaff?

1056 Mr. {Schaaff.} Sony is also very supportive of such  
1057 legislation and we would be very happy to participate and  
1058 help in the formation of that legislation.

1059 Mr. {Olson.} All right. Thank you. And Ms.  
1060 Fitzgerald, this is just for you, but why did you choose to  
1061 contact law enforcement, the FBI, and the Secret Service as  
1062 soon as you became aware of the incident? And is this a  
1063 typical response for Epsilon to get law enforcement involved  
1064 when a breach occurs when you don't necessarily know the  
1065 extent of it?

1066 Ms. {Fitzgerald.} Well, we knew pretty quickly that  
1067 there had been some data that had been downloaded and taken  
1068 by somebody who wasn't authorized, and therefore, it was a  
1069 criminal act in our mind. And so we went to look for law  
1070 enforcement, the right ones to help us go after the bad guys.

1071 Mr. {Olson.} Okay. And for you, Mr. Schaaff? I know  
1072 you and PlayStation had one heck of an April. But why did  
1073 you conclude that notifying PlayStation Network customers via  
1074 the PlayStation blog was, as you stated, ``one of the best,  
1075 fastest, and most direct means of communicating with  
1076 customers?''

1077 Mr. {Schaaff.} In the years that PlayStation has been  
1078 in business, we have managed this blog and it has become a  
1079 very, very popular source of information for our customers  
1080 about new game titles and all kinds of information related to  
1081 PlayStation. And we know that it is a good way to get a  
1082 message out to customers quickly. Of course, that wasn't the  
1083 only way we communicated with our customers. We did follow  
1084 up with public announcements through other channels, as well  
1085 as email, direct emails to the consumers following the  
1086 breach.

1087 Mr. {Olson.} Okay. And one final question about sort  
1088 of how you are prepared for this. I mean I know, Ms.  
1089 Fitzgerald, for your testimony Epsilon had reactive plans in

1090 place ready to go if some sort of breach happened, and I  
1091 assume that is the same for Sony.

1092 Mr. {Schaaff.} Absolutely.

1093 Mr. {Olson.} But, I mean, is there a specific entity  
1094 within both of your companies that is proactive? I mean  
1095 somebody you have got in your company that sort of looks at  
1096 your security systems and tries to penetrate it, tries to  
1097 find the weaknesses; I mean sort of a proactive approach  
1098 instead of reacting to a breach, preventing a breach by  
1099 recognizing weaknesses within the company?

1100 Mr. {Schaaff.} We have a successful approach the  
1101 security involved both proactive as well as reactive  
1102 approaches, and we definitely have those kinds of resources  
1103 in place in my company and in Sony Corporation as a whole, an  
1104 important part of our process.

1105 Ms. {Fitzgerald.} And I would agree with that also.  
1106 Epsilon has that.

1107 Mr. {Olson.} Okay. I see I am down to 16 seconds. I  
1108 thank the witnesses again for your time. And at the risk of  
1109 getting crosswise with the chairwoman and Mr. Stearns left,  
1110 but go Mavericks.

1111 Mr. {Schaaff.} Thank you.

1112 Mrs. {Bono Mack.} The chair recognizes Mr. Harper for 5  
1113 minutes.

1114 Mr. {Harper.} Thank you, Madam Chair. I would ask you,  
1115 Mr. Schaaff, why did it take Sony approximately 7 days to  
1116 notify customers that their personal data had been  
1117 compromised?

1118 Mr. {Schaaff.} Well, the basic essence here was the  
1119 find the right balance between notifying customers as soon as  
1120 we had some sense that something had gone wrong but not being  
1121 irresponsible in that notification and creating undue stress  
1122 or concern within the customer base. We immediately began an  
1123 investigation and we were able to notify customers within a  
1124 couple of days that we had had an unauthorized external  
1125 intrusion. But it took us several more days to be able to  
1126 clearly discern what information had been taken and even at  
1127 that point, we were not able to rule out the possibility that  
1128 credit card information had been taken. Nevertheless, we  
1129 went ahead and made a public statement regarding the  
1130 potential of those losses.

1131 Mr. {Harper.} I just want to be clear. So how long was  
1132 it before any customers got notification?

1133 Mr. {Schaaff.} We first discovered unusual activity on  
1134 the 19th. We shut down the network on the 20th of April, and  
1135 we notified consumers on the 22nd of April. So it was  
1136 basically 2 days.

1137 Mr. {Harper.} Did you notify all the consumers at that

1138 point?

1139 Mr. {Schaaff.} Well, so at that point we were intensely  
1140 involved in this investigation to try to figure out what to  
1141 notify the customers about. And so at that time we notifying  
1142 using the blog that we believed that there had been an  
1143 intrusion. And then beginning on the 26th when we made a lot  
1144 of public announcements related to specific information that  
1145 may have been lose we initiated through news channels,  
1146 obviously our blog, as well as through a direct email  
1147 campaign to the customers detailed information about the  
1148 nature of the loss.

1149 Mr. {Harper.} How many notifications did each consumer  
1150 receive?

1151 Mr. {Schaaff.} Well, my understanding is that in regard  
1152 to the Sony PlayStation breach, that should have been  
1153 approximately 77 million emails that were sent.

1154 Mr. {Harper.} Now, I understand but were they notified  
1155 more than one time as you learned additional information?

1156 Mr. {Schaaff.} Well, we notified via the blog on the  
1157 22nd. We provide updates on that blog on a regular basis as  
1158 to kind of the concurrent state of affairs, but I believe in  
1159 terms of the email notifications related to the potential  
1160 loss of data, that was a one-time event.

1161 Mr. {Harper.} Do you believe the news that you passed

1162 on, looking back now, do you believe it was done quickly  
1163 enough?

1164 Mr. {Schaaff.} What I would say is that we tried very,  
1165 very hard to find the right balance there, and I believe that  
1166 if we had responded earlier, it would have probably been  
1167 irresponsible. Even to this day we question whether we  
1168 should have taken a little bit more time to finish the  
1169 investigation with regard to the credit card information. I  
1170 believe we probably struck the right balance, but it was a  
1171 tough call.

1172 Mr. {Harper.} And I know there was a letter that was  
1173 sent out on May 3 where you had indicated that there was no  
1174 evidence of misuse of the customers' personal information  
1175 that was accessed during that breach. We are a month past  
1176 that point. Is that still your position on that?

1177 Mr. {Schaaff.} When we talked to the credit card  
1178 companies, they have still told us that they see no signs of  
1179 unusual activity related to this breach.

1180 Mr. {Harper.} And do you know where the attacks  
1181 originated?

1182 Mr. {Schaaff.} Unfortunately, at this time we don't.

1183 Mr. {Harper.} Okay.

1184 Mr. {Schaaff.} I mean we are working with law  
1185 enforcement and others to try to figure that out, but at this

1186 time we don't have any clear--

1187 Mr. {Harper.} Of course, you know we certainly hear  
1188 media reports or speculation, and I know you don't have it  
1189 with any certainty, but there was one report that initially  
1190 suggested that Amazon's pay-per-use cloud service may have  
1191 been used. Is there any accuracy to that or any proof of  
1192 that?

1193 Mr. {Schaaff.} Well, so what I know is the FBI is  
1194 investigating that report, and at this time I don't have any  
1195 other information about whether that is true or not.

1196 Mr. {Harper.} Now, does Sony Online Entertainment and  
1197 Sony Network Entertainment, are they using the same server  
1198 models and security protections and the software?

1199 Mr. {Schaaff.} We comply with the same types of  
1200 industry practices and are subject to the same policies as  
1201 far as being a part of the Sony Corporation. The specific  
1202 architecture of each of those services is probably different  
1203 because the types of services that we provide are different.  
1204 But, you know, across the industry, most internet service  
1205 providers are building their services out of largely the same  
1206 basic components so there is probably a lot of commonality  
1207 there.

1208 Mr. {Harper.} Thank you. Madam Chair, I yield back the  
1209 balance of my time.

1210 Mrs. {Bono Mack.} I thank the gentleman. And at this  
1211 point in time we are going to recess the committee to head  
1212 over to the floor for vote. And our intention is to return  
1213 as soon after as we can from the series of votes. It should  
1214 be about 45 minutes is my guess. Things could change. So  
1215 the subcommittee stands recessed until after the last vote on  
1216 the floor.

1217 Ms. {Fitzgerald.} Thank you.

1218 [Recess.]

1219 Mrs. {Bono Mack.} The subcommittee will reconvene and  
1220 come to order obviously. I wanted to thank you very much for  
1221 indulging us and apologize that there has been a slight  
1222 little change of plans with the minority headed over to the  
1223 White House for a very important meeting with the President.  
1224 We have agreed that we would conclude questions.

1225 But before I do that, I would like to offer the two of  
1226 you the opportunity to give us any final thoughts you might  
1227 have and any recommendations for legislation as we move  
1228 forward in the process here. So I recognize each of you for  
1229 5 minutes to do that. And you don't have to take the full 5  
1230 minutes if you would like, but the time is yours if you would  
1231 like it.

1232 Ms. {Fitzgerald.} Thank you. Honestly, as we have  
1233 thought about this, we would greatly appreciate the

1234 opportunity to work with you and your staff and any members  
1235 of your subcommittee to create a national data breach  
1236 notification standard. The details within it would have to  
1237 be worked out as we think through what would be all the  
1238 ramifications. And I think clearly I would not be the only  
1239 one with experience, but we would love to work with that on  
1240 you.

1241 Mrs. {Bono Mack.} Mr. Schaaff?

1242 Mr. {Schaaff.} Thank you. I want to thank you again  
1243 for the opportunity to come and speak today and especially  
1244 thank you for all the work you have done related to  
1245 intellectual property protection. This is a really critical  
1246 part of the work we are trying to do to build and grow our  
1247 business.

1248 As you heard in our testimony today and in the private  
1249 session where we shared more technical details regarding the  
1250 breach yesterday, despite taking what we believe to be  
1251 extremely appropriate and substantial steps to build a safe  
1252 and protected network, hackers were able to get into the  
1253 network. The thing that is frightening about this is it is  
1254 easy to focus on Sony and look at the things that we might be  
1255 able to do in the future to strengthen our network, but the  
1256 reality is because we are all building our networks out of  
1257 the same basic ingredients, if there is a weakness in the way

1258 that we have built things, chances are, the weaknesses may  
1259 lie in the components that we rely on from the variety of  
1260 vendors that we all build our products out of. And I think  
1261 that we are working together as industry to try to strengthen  
1262 our processes and our practices and our technologies, but I  
1263 think the conclusion that I would leave you with today is  
1264 that without further assistance from the government, I think  
1265 that we are all going to have a world of hurt in this  
1266 internet economy. And we really would appreciate and request  
1267 your assistance.

1268           And regarding the specific legislation, we are also  
1269 extremely supportive of this and would welcome the  
1270 opportunity to contribute and speak to you further regarding  
1271 its development. Thank you.

1272           Mrs. {Bono Mack.} Well, I thank you both very much.  
1273 And Mr. Schaaff, I would also like to address a comment  
1274 earlier about the question of would you or would you not file  
1275 suit again to protect your intellectual property, and I  
1276 wanted to commend you on your answer. And I am glad that you  
1277 did it then. And you know, too often people are afraid of  
1278 being hacked and the retribution because of the decisions you  
1279 make.

1280           Mr. {Schaaff.} It can be a lonely place.

1281           Mrs. {Bono Mack.} Well, I want to applaud you for that.

1282 And again, thank you both very much for the spirit with which  
1283 you came before us today and the spirit of cooperation. I  
1284 think the committee is very excited about the opportunity to  
1285 work with you and to craft good legislation.

1286 So we have a unique opportunity now as a subcommittee to  
1287 make certain that the future cyber attacks on American  
1288 consumers will never again be a silent crime.

1289 So at this point I would like to remind all members they  
1290 have 10 business days to submit questions for the record, and  
1291 I ask witnesses to please respond promptly to any questions  
1292 they receive. And the hearing is now adjourned.

1293 Mr. {Schaaff.} Thank you very much.

1294 Ms. {Fitzgerald.} Thank you very much.

1295 [Whereupon, at 2:14 p.m., the subcommittee was  
1296 adjourned.]