1   NEAL R. GROSS & CO., INC.

2   RPTS SHIPLE

3   HIF334020

4

5

6   IDENTITY VERIFICATION IN A POST-BREACH WORLD

7   THURSDAY, NOVEMBER 30, 2017

8   House of Representatives

9   Subcommittee on Oversight and Investigations

10 Committee on Energy and Commerce

11 Washington, D.C.

12

13

14

15   The subcommittee met, pursuant to call, at 10:15 a.m., in

16 Room 2322 Rayburn House Office Building, Hon. Greg Walden

17 [chairman of the subcommittee] presiding.

18   Members present: Representatives Walden (ex officio),

19 Griffith, Brooks, Collins, Walberg, Costello, Carter,

20 Schakowsky, Castor, Tonko, Clarke, Ruiz, and Pallone (ex

21 officio).

22   Staff present: Jennifer Barblan, Chief Counsel, Oversight

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

23   & Investigations; Samantha Bopp, Staff Assistant; Adam Fromm,

24   Director of Outreach and Coalitions; Ali Fulling, Legislative

25   Clerk, Oversight & Investigations, Digital Commerce and Consumer

26   Protection; Elena Hernandez, Press Secretary; Paul Jackson,

27   Professional Staff, Digital Commerce and Consumer Protection;

28   Bijan Koohmaraie, Counsel, Digital Commerce and Consumer

29   Protection; Alex Miller, Video Production Aide and Press

30   Assistant; John Ohly, Professional Staff, Oversight &

31   Investigations; Hamlin Wade, Special Advisor, External Affairs;

32   Jessica Wilkerson, Professional Staff, Oversight &

33   Investigations; Greg Zerzan, Counsel, Digital Commerce and

34   Consumer Protection; Julie Babayan, Minority Counsel; Jeff

35   Carroll, Minority Staff Director; Chris Knauer, Minority

36   Oversight Staff Director; Miles Lichtman, Minority Policy

37   Analyst; Dino Papanastasiou, Minority GAO Detailee; and C.J.

38   Young, Minority Press Secretary.

39   Mr. Griffith. We will go ahead and get started.

40   Welcome to this meeting of the O&I Subcommittee of Energy

41 and Commerce. So that everybody knows, there are a lot of folks

42 who are at another hearing downstairs and will be drifting in and

43 out.

44   Also, I would like to take a point of personal privilege and

45 recognize Allie Gilmer and Olivia Smoot who are here visiting

46 today from my district at Auburn High School in Riner, Virginia.

47   They are too young to remember this but I started

48 representing the Riner area in 1994 in the state legislature. So

49 it's good to --

50   Ms. Castor. Do you want to stand up?

51   Mr. Griffith. Yes, stand up. Be recognized. Thank you.

52   Thank you again. Welcome. Glad you're here with us today.

53   That being said, let's get started with our business here

54 today and other folks will join us as we go forward on this very

55 important issue.

56   We are here today to talk about a very important topic,

57 identity verification in a post-breach world. This hearing is

58 especially timely, given several events that have taken place

59 since the hearing itself was announced last week, including three

60 newly-discovered data breaches that comprised an additional 58.7

61　million records as well as two major shopping days -- Black Friday

62　and Cyber Monday.

63　　　With consumers rushing to take advantage of holiday sales

64　both in stores and online, the questions and challenges around

65　modern identity verification become even more pressing.

66　　　Data breaches have been increasingly -- have been an

67　increasing problem over the last several years. In fact, it is

68　likely that everyone in this room has had their information

69　included in a recent breach.

70　　　Between the 57 million accounts comprised in Uber's recent

71　disclosed 2016 breach, the 145 million accounts compromised in

72　Equifax's breach, or the 22 million accounts compromised in the

73　OPM breach as well as many others, I would argue that it would

74　be difficult to find an American whose information has not been

75　compromised.

76　　　While these breaches themselves are troubling enough, they

77　also raise a subtle more complicated series of questions and

78　issues around the ways in which organizations including

79　government agencies, banks, health care organizations, and retail

80　companies perform identity verification of their citizens and

81　their customers.

82　　　It is a well understood concept that, to quote the famous

83   cartoon on the internet, nobody knows you're a dog when you're

84   in the internet.

85   This anonymity has many advantages and it is important to

86   many aspects of the modern internet.

87   However, as the global economy has become more and more

88   digital and an increasing amount of commerce takes place online,

89   it also creates significant challenges for organizations

90   attempting to ensure that they provide information and services

91   only to authorized individuals.

92   Because these interactions usually take place on opposite

93   ends of an internet connection with participants rarely if ever

94   meeting face to face, the ability of organizations to remotely

95   verify individuals has been a constant struggle.

96   As a result, for years many organizations have relied on a

97   type of identity verification known as knowledge-based

98   authentication, or KBA. We are all familiar with this process

99   even if we don't quite know it.

100   For example, some online accounts ask consumers to provide

101   answers to security questions such as their mother's maiden name,

102   the make and model of their first car, or the street on which they

103   grew up on.

104   Similarly, when consumers attempt to open new credit lines

105   they are often asked a series of multiple choice questions that

106   may ask who provided a consumer loan and in what year.

107   These are all examples of KBA. The effectiveness of KBA

108   depends on a very important assumption -- that information such

109   as birthdays, mothers' maiden names, addresses, work histories

110   and other KBA attributes remain relatively secret.

111   In today's post-breach world, this is a tenuous assumption.

112   Add the wealth of personal information consumers voluntarily

113   share about their lives through social media and this assumption

114   appears almost laughable.

115   So what do we do? If modern commerce and many other services

116   including government services rely on KBA for identity

117   verification and that verification is no longer as secure or

118   reliable as it was in the past, we need new strategies and new

119   technologies to ensure that consumers are protected and economic

120   growth continues and we need them quickly.

121   With the exponential growth of connected devices and

122   services, it is likely that we will see more data breaches more

123   often, not less.

124   Luckily, we are not starting from scratch. In the public

125   sector, the National Institute for Standards in Technology -- NIST

126   -- spent the past several years developing strategies and

127   frameworks for identity verification under their Trusted

128   Identities Group -- TIG.

129   As a part of this work, NIST's TIG has provided funding to

130   pilot programs looking to develop, implement, and leverage

131   innovative new technologies that move organizations beyond KBA.

132   Similarly, in the private sector, many companies and

133   organizations from a wide variety of sectors have come together

134   to create the Fast Identities Online, or FIDO, Alliance.

135   The FIDO Alliance provides a forum for collaboration and

136   cooperation around the development of standards-based

137   interoperable technologies. These standards are freely

138   available and already deployed in the products of companies like

139   Google and PayPal.

140   Our witnesses today will not only help us understand the

141   cumulative impact of the dozens of data breaches that have

142   occurred in recent years go also assess how current practices can

143   and should be improved to protect consumers and their information

144   and how it's been breached.

145   Today's hearing is the start of what I expect will be a much

146   longer conversation. But it's a necessary conversation to have

147   as our world becomes ever more connected. Identity verification

148   is a challenge that will only continue to grow.

149   Thank you, and I yield back and now recognize Ms. Castor of

150   Florida for an opening statement.

151   Ms. Castor. Well, thank you, Mr. Chairman, and thank you

152   for calling this hearing.

153   Mr. Chairman, data breaches are compromising the personal

154   information of millions of Americans. The Equifax breach earlier

155   this year, for example, exposed the personal information

156   including names, Social Security numbers, birth dates, addresses,

157   and other sensitive data of as many as 145 million Americans.

158   And there have been many more -- Yahoo, JPMorgan Chase, eBay,

159   Uber. We simply cannot accept this as standard operating

160   procedure. When companies like Equifax, Yahoo, and Uber fail to

161   protect the vast information they collect about consumers, it

162   poses very serious risks.

163   It's not limited to private corporations. Governmental

164   entities have also failed to adequately protect personal private

165   data.

166   But with each data breach after each data breach,

167   compromising more and more of consumers' personal information,

168   we have got to ask how do we ensure an online identity can be

169   verified only by the person in question.

170   I also think it's important that we not forget that companies

171   should be held accountable when they fail to protect our data.

172   The Equifax breach exposed the personal information of

173   nearly half of the American population and it could have been

174   prevented by applying basic security standards.

175   So what is the recourse? What is the appropriate recourse?

176   I know that experts are working to develop methods to better

177   protect online identities and I would like to hear what your

178   recommended solutions are.

179   Under President Obama, the White House released the National

180   Strategy for Trusted Identities in Cyberspace. It's a framework

181   for public and private collaboration on protecting digital

182   identities and improving online transactions.

183   So building on that effort, companies have begun

184   experimenting with ways to improve identity verification and

185   authentication.

186   I would like to hear about some of these solutions as well

187   as what we can do to protect consumers' privacy. As more and more

188   of our lives are online, it is equally important that we ensure

189   that these systems are secure and that the ways in which we access

190   these systems are protected.

191   I would like to thank our witnesses -- Mr. Jeremy Grant, Mr.

192   Troy Hunt, Mr. Ed Mierzwinski -- for coming today to discuss 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.

10

193 principles and various challenges in verifying online identities.

194 Each of you brings a wealth of knowledge and experience to

195 this hearing and it's a pleasure to have you here today. Thank

196 you, and I yield back.

197 Mr. Griffith. I thank the gentlelady.

198 I now recognize the chairman of the full committee, Mr.

199 Walden of Oregon.

200 The Chairman. I thank the chairman, and we appreciate your

201 leadership on this and so many other issues, and we want to thank

202 the witnesses for being here today.

203 We have another hearing going on downstairs on the

204 anniversary of the 21st Century Cures legislation so I am bouncing

205 back and forth today.

206 Today's hearing is about the future of digital commerce, as

207 we all know, and it's about the future of how we ensure the person

208 on the other end of an online transaction is in fact the person

209 they claim to be. What a concept.

210 For years, we have relied on user names, passwords, and

211 knowledge-based questions to confirm a user's identity. It's not

212 a particularly sophisticated process. Your mother's maiden name

213 or the make and model of your first car aren't exactly reliable

214 forms of verification.

215   Regardless, this process was suitable for a period of time

216   in the evolution of our connected world but that time has long

217   since passed, as we all know.

218   As noted by one of our witnesses today, it was almost a decade

219   ago that the 2008 Commission on Cybersecurity for the 44th

220   presidency highlighted identity as a frequent attack vector for

221   cyberattacks.

222   This prompted the previous administration to launch the

223   National Strategy for Trusted Identities in Cyberspace, or NSTIC.

224   As we will hear today, this high-level federal attention

225   encouraged the progress but we still have a long ways to go.

226   How far? Well, according to Verizon's annual data breach

227   investigation report, about 80 percent of breaches last year used

228   identity as a point of compromise -- 80 percent.

229   What has changed to make existing identity management

230   practices so ineffectual and vulnerable to attack? There are a

231   number of factors at play but the underlying answer is fairly

232   simple.

233   Today, the information necessary to compromise identity is

234   readily available to those who wish to find it. We live in a

235   post-breach world. Just look at the massive breaches that have

236   occurred over the last several from Target and Home Depot to Yahoo,

237   Anthem OPM, Equifax and, most recently, Uber, to name a few.

238   I would be surprised if anyone in this room has not had at

239   least some portion of their personal details stolen in the last

240   two years, let alone their digital lifetime.

241   I remember a former colleague from Michigan who chaired the

242   Intelligence Committee, Mike Rogers, used to say there are two

243   types of companies in America -- those that know they've been

244   breached and those that don't.

245   It is not, however, just stolen data that undermines current

246   identity verification practices. The explosion of social media

247   is also a factor.

248   Every day, consumers voluntarily post, tweet, and share

249   details about their lives, adding to the rich data set of

250   information available to malicious actors.

251   One of our witnesses, Mr. Hunt, is a global expert on these

252   issues and that's why your testimony is so very valuable to our

253   work, especially on how bad actors can compromise identity through

254   the collection of personal information and data that already

255   exists in the digital universe.

256   He endured a 27-hour journey to be here, I am told, and I

257   suspect his testimony will be illuminating for all of us. I

258   thought I had a long trip back and forth to the West coast every

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

13

259   week.

260   We can no longer ignore the current reality. Whether

261   through theft or voluntary disclosure, our information is out

262   there and this is not likely to change.

263   Social media will continue to grow. Social, cultural, and

264   economic benefits are just too great for it not to. Likewise,

265   digital commerce and online transactions are integral to our

266   economic prosperity both now and in the future.

267   As our lives become increasingly entwined in the digital --

268   with the digital space, this must come with an acceptance that

269   our information will always be at risk.

270   Such is the nature of the cyber threat we face and there is

271   no perfect security in the connected world. But that makes it

272   even more important that we find ways to reduce vulnerabilities

273   in our digital ecosystem.

274   Clearly, identity is one of those weaknesses. So therefore,

275   I look forward to the work this committee is doing and the

276   testimony you all have submitted to us and the policies that will

277   develop, moving forward.

278   With that, Mr. Chairman, I yield back the balance of my time

279   and, again, thank your witnesses for being here and, as I said,

280   I've got a couple of these I have to bounce between. But we

281   appreciate the work you're doing.

282   Mr. Griffith. Thank you, Mr. Chairman. I appreciate that.

283   I will tell you that Mr. Hunt not only sacrificed with the

284   27-hour flight to get here but also put on a suit and tie for us

285   where he normally wears jeans and a black t-shirt, according, at

286   least to his comments on the internet.

287   [Laughter.]

288   Mr. Griffith. But anyway --

289   The Chairman. I was starting to wonder if it's actually him

290   or a stolen identity before that. But I don't know. Thank you.

291   Mr. Griffith. Anyway, thank you, Mr. Chairman.

292   At this point, I would ask -- oh, I would recognize Mr.

293   Pallone of New Jersey for an opening statement. Glad you made

294   it. Thank you.

295   Mr. Pallone. Thank you, Mr. Chairman.

296   I want to -- I have actually got the wrong statement here

297   from the other committee.

298   Mr. Griffith. We will give you a minute. We have explained

299   to everybody that we have two hearings going on at the same time

300   and that folks are having to bounce back and forth so --

301   Mr. Pallone. All right.

302   So let me, again, thank you, 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.

303   So much of our lives today is linked to what we do online

304   and companies in virtually every sector of the economy collect

305   vast amounts of personal data about consumers, and these companies

306   know they are targets for malicious attacks and all too often they

307   fail to protect the valuable consumer information they collect

308   and store.

309   For example, recently the ride service company Uber revealed

310   that it had been hacked more than a year ago, and this breach

311   reportedly exposed the personal information of 57 million riders

312   and drivers.

313   This security breach is yet another example of a company that

314   failed to protect the data of its customers and then failed to

315   come clean about their security breach, in this case for more than

316   a year.

317   Then there was the Equifax data breach which compromised the

318   personal data of more than 145 million Americans, and what's

319   worse, the Equifax breach compromised personal data like Social

320   Security numbers and birth dates that are difficult or impossible

321   to change.

322   And consumers affected by the Equifax breach are vulnerable,

323   particularly because these identity verifiers can give someone

324   access to other sensitive 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.

325   The committee is still waiting for answers to questions we

326   asked Equifax both before and after our hearing on the breach and,

327   obviously, that's unacceptable so, hopefully, we will get

328   answers.

329   It's also unacceptable to the American people because when

330   companies fail to protect consumer data consumers pay the price,

331   sometimes years after a breach.

332   So as data breaches continue to compromise our personal

333   information, it's important that we explore how consumers and the

334   holders of consumer information can verify that individuals are

335   who they say they are online.

336   For example, how many times has each of us been asked to

337   provide the last four digits of our Social Security number to get

338   access to other information?

339   But how do we protect consumers' digital identities,

340   especially after the Equifax data breach exposed the Social

341   Security numbers of nearly half the U.S. population.

342   And as companies suggest that they may move to behavioral

343   and biometric verifiers, are we comfortable with how much more

344   personal information will be collected and used?

345   Are we comfortable with trusting that companies will keep

346   this data secure? And these are important questions now facing

347 the world of digital commerce.

348   According to the Identity Theft Resource Center, as many as

349 1,190 data breaches have occurred so far this year. Any data

350 breach exacerbates the issues the public is facing in verifying

351 their identities and authenticating access online.

352   Hackers and other malicious actors erode the trust we have

353 online by using the data they've been able to glean about each

354 and every one of us, and that's not good for business and it's

355 certainly not good for consumers.

356   So, again, I just want to thank our witnesses for being here

357 today to discuss the latest in identity verification and the

358 challenges of protecting people's data and I believe that unless

359 we act and pass meaningful legislation we will continue to see

360 more data breaches and the unfortunate ripple effects that result

361 from them.

362   I don't know if -- you don't want to add anything? All right.

363 I yield back, Mr. Chairman.

364   Mr. Griffith. Thank you very much for yielding back. I

365 appreciate that, Ranking Member.

366   With that being said, I would now ask for unanimous consent

367 that the members' written opening statements be made a part of

368 the record. Without objection, they will be so entered.

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

369   I would now like to introduce our panel of witnesses for

370   today's hearing and appreciate all of you being here.

371   First, we have Mr. Troy Hunt, the information security author

372   and instructor for Pluralsight. Next is Mr. Jeremy Grant, who

373   serves as the managing director of Technology Business Strategy

374   at Venable. And finally, we have Mr. Ed Mierzwinski, who is the

375   consumer program director at U.S. PIRG, or PIRG.

376   Thank you all for being here today and I look forward to your

377   testimony and we appreciate you providing that testimony. We

378   look forward to the opportunity to discuss identity verification

379   with you all.

380   As you all are aware, the committee is holding an

381   investigative hearing and when doing so it is the practice of this

382   committee -- this subcommittee of taking that testimony under

383   oath.

384   Do any of you have an objection to testifying under oath?

385   Seeing none, the chair then advises you that under the rules

386   of the House and the rules of this committee, you are entitled

387   to be accompanied by counsel.

388   Do any of you desire to be accompanied by counsel during your

389   testimony today?

390   Seeing no request for counsel, in that case would you please

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

391   rise and raise your right hand, and I will swear you in.

392   [Witnesses were sworn.]

393   Seeing affirmative answers from all, you are now under oath

394   and subject to the penalties set forth in Title 18 Section 1001

395   of the United States Code.

396   You may now give a five-minute summary of your written

397   statement and we will begin with you, Mr. Hunt.

398   Thank you so much for being here. You have five minutes.

```
399    STATEMENTS OF TROY HUNT, INFORMATION SECURITY AUTHOR AND

400    INSTRUCTOR, PLURALSIGHT; JEREMY A. GRANT, MANAGING DIRECTOR,

401    TECHNOLOGY BUSINESS STRATEGY, VENABLE, LLP; ED MIERZWINSKI,

402    CONSUMER PROGRAM DIRECTOR, U.S. PIRG

403

404    STATEMENT OF MR. HUNT

405         Mr. Hunt.  Vice Chairman Griffith, Ms. Castor, and

406    distinguished members of the House Energy and Commerce Committee,

407    thank you for the opportunity to testify today.

408         My name is Troy Hunt.  I am an independent information

409    security author and instructor for Pluralsight.  I am also the

410    creator of data breach notification service known as Have I Been

411    Pwned.

412         In my time running this service, I've analyzed hundreds of

413    individual data breaches containing many billions of records and

414    I've observed first hand both the alarming increase in incidents

415    and, indeed, the impact they are having on people's lives.

416         This testimony draws on my experiences running the service

417    and describes the challenges we are now facing in a time where

418    data breaches have become the new normal.

419         When we talk about data breaches, we are really talking about

420    a range of different types of events that can lead to the exposure
```

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

21

421   of their personal information.

422   We typically think of malicious actors exploiting

423   vulnerabilities and protected systems and, indeed, that's an

424   enormous prevalent and alarming situation.

425   But increasingly we also see data breaches occur as a result

426   of simple human error. For example, accidentally publishing data

427   to an unprotected publicly-facing server where it's then

428   discovered by intended parties.

429   We have a perfect storm of factors that are causing both the

430   frequency and scale of these incidents to accelerate. Cloud

431   services have made it easier than ever to publish data publicly,

432   and that has helped to drive the expansion of other online

433   services, which have in turn increased the overall attack surface

434   of the internet.

435   At the same time, we have the rapidly growing internet of

436   things, collecting classes of data we simply never had digitized

437   in the past and, increasingly, we are seeing that information

438   appear in data breaches, too.

439   Organizational attitudes to our personal information lead

440   to data maximization. That is a desire to collect as much of it

441   as possible, often well beyond the scope of what is actually needed

442   by the service it's being provided 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.**

22

443   Frequently, this is without informed consent, particular by

444 the likes of data aggregators and, indeed, we have seen them suffer

445 data breaches, too, both here in the U.S. and overseas.

446   Now, data is viewed as an asset yet organizations fail to

447 recognize that it is also a liability. Exacerbating exposure of

448 data is a rampant trading scene. Data is not only sold for profit

449 but regularly exchanged by individuals building personal

450 collections.

451   I liken it to kids exchanging baseball cards, except that

452 unlike trading a physical commodity, the exchange of data breaches

453 is more like making a photocopy, as the original version still

454 exists.

455   Once it enters circulation, it is impossible to contain it.

456 The data breach genie is out of the bottle. We are also learning

457 how much we don't know as significant data breaches that occurred

458 years ago come to light.

459   We have no idea how many more unknown incidents are out there,

460 and not only do we not know which organizations have lost their

461 data and are unaware of it themselves, we don't know which ones

462 are deliberately concealing data breaches.

463   There is a lack of accountability when a breach does occur.

464 We know this because very little changes in the industry

465   afterwards.

466   We constantly see large data breaches and people ask, will

467   this be the watershed moment where we start taking these breaches

468   more seriously.

469   Yet, nothing changes and we merely repeat the same discussion

470   after the next incident. We are also disclosing large amounts

471   of personal data of our own free will, such as our date of birth,

472   by social media.

473   We think nothing of it because a growing proportion of the

474   population has never known a time where we didn't do this. They

475   are the internet natives that have grown up in an environment of

476   personal information sharing.

477   Consider the impact on knowledge-based authentication, the

478   very premise that there is information that you know that is

479   sufficient to prove your identity.

480   Mr. Griffith. All right. Mr. Hunt, I apologize to knocking

481   you off but we have gotten word from our technical folks that the

482   microphone is not close enough to your mouth and we need that.

483   I can hear you fine but apparently the folks recording this

484   for later cannot. So --

485   Mr. Hunt. I will continue from here, a little bit closer.

486   Mr. Griffith. Thank you, sir.

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

24

487   Mr. Hunt. Consider the impact on knowledge-based

488   authentication, the very premise that there is information that

489   you know that is sufficient to prove your identity. That same

490   information is increasingly public.

491   My dad recently had some help setting up a new broadband

492   connection, and after calling up the provider the first thing they

493   asked him was his date of birth. That's the same personal

494   attribute I had exposed after I donated blood and that

495   subsequently appeared in a data breach.

496   And that is really the challenge we have today, the premise

497   of authenticating one's self with information that only they

498   should know, yet is increasingly in the public domain.

499   That worked years ago when information was contained in a

500   small number of silos but that's not the world we live in today.

501   And consequently, our assumption about who knows what has to

502   change accordingly in the age of the data breach.

503   Thank you very much.

504   [The prepared statement of Mr. Hunt follows:]

505

506   **********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.

507   Mr. Griffith. Thank you. I appreciate that, and now

508   recognize Mr. Grant. Yes, got to turn on the mic.

509   Mr. Grant. Let's me try that again.

510   Mr. Griffith. There you go.

511   STATEMENT OF MR. GRANT

512

513   Mr. Grant. Good morning, Vice Chairman Griffith, Ms.

514   Castor, members of the committee. Thank you for the opportunity

515   to discuss identity with you today.

516   As background, I've worked for more than 20 years in both

517   industry and government at the intersection of identity and

518   cybersecurity.

519   In 2011, I was selected to lead the National Strategy for

520   Trusted Identities in Cyberspace, or NSTIC, which was a White

521   House initiative focused on improving security, privacy, choice,

522   and innovation online for better approaches to digital identity.

523   In that role, I built out what is now the Trusted Identities

524   Group at the National Institute of Standards and Technology and

525   also served as NIST's senior executive advisory for identity

526   management.

527   I left government in 2015 and now lead the Technology

528   Business Strategy practice at Venable, a law firm with the

529   country's leading privacy and cybersecurity practice, though I

530   should note today my testimony represents my views alone.

531   So let me say up front I'm quite grateful to the committee

532   for calling this hearing today. Identity is a topic that impacts

533 every American but it's only recently that identity has started

534 to get proper attention from policy makers in the U.S., and at

535 a high level the way that we handle identity in America impacts

536 our security, our privacy, and our liberty.

537 From an economic standpoint, particularly as we start to move

538 high-value transactions into the digital world, identity can be

539 the great enabler, providing the foundation for digital

540 transactions and online experiences that are more secure, more

541 enjoyable for the user and, ideally, more respectful with their

542 privacy.

543 When we don't get identity right we enable a great set of

544 attack points for criminals and other adversaries looking to

545 execute attacks in cyberspace and, unfortunately, we have not been

546 doing very well here.

547 Last year, a whopping 81 percent of hacking attacks were

548 executed by taking advantage of weak or stolen passwords.

549 Eighty-one percent is an enormous number.

550 It means that it is an anomaly when a breach happens and

551 identity does not provide the attack factors and, as my colleague,

552 Troy, will probably discuss today with his website, Have I Been

553 Pwned, there is now billions of compromised usernames and

554 passwords that are out there in the marketplace. It is high time

555   we find a way to kill the password.

556   Outside of passwords, we have seen adversaries go after

557   massive datasets of Americans in large part so they have an easier

558   time compromising the questions used in identity verification

559   tools like KBA.

560   This was illustrated quite vividly by the 2015 hack of the

561   IRS' Get My Transcript application where more than 700,000

562   Americans had sensitive tax data compromised.

563   A key takeaway for this committee to understand today is that

564   attackers have caught up with many of the first generation tools

565   that we have used to protect and verify identity.

566   The recent Equifax breach might have driven this point home

567   but the reality is that these tools have been vulnerable for quite

568   some time.

569   There are many reasons for this and there is certainly blame

570   to allocate. But the most important question at this point is

571   what should government and industry do about it now.

572   As I lay out today, I believe the government is going to need

573   to step up and play a bigger role to help address critical

574   vulnerabilities in our digital identity fabric.

575   There are five primary areas where government, working

576   together with the private sector, can help address the weaknesses

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

577   of first generation identity verification and authentication

578   tools and deliver next-generation solutions that are not only more

579   secure but also better for privacy and consumer experiences.

580   First, when talking about the future of the Social Security

581   number and whether it needs to be replaced, it is essential for

582   folks to understand the difference between SSN's role as an

583   identifier and its use as an authenticator.

584   SSN should no longer be used as authenticators but that does

585   not mean we need to replace them as identifiers. Instead, let's

586   just try treating like the widely available numbers that they are.

587   That means that as a country we stop pretending that

588   knowledge of somebody's Social Security number can actually be

589   used to prove that they are who they claim to be.

590   Second, along with the SSN let's just recognize how useless

591   passwords have become as a security tool. There is no such thing

592   as a strong password in 2017 and we should stop trying to pretend

593   otherwise.

594   Third, recognize that it's not all bad news out there.

595   Government and industry have recognized the problem with old

596   authenticators like passwords and SSNs and they've actually been

597   working together the last few years to make strong authentication

598   easier.

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

599   Multi stakeholder efforts like the FIDO Alliance, which Vice

600   Chairman Griffith mentioned earlier, have developed standards for

601   next-generation authentication that are now being embedded in

602   most devices, operating systems, and browsers in a way that

603   enhances security, privacy, and user experience. The government

604   can play a role in helping to drive user adoption.

605   Fourth, while authentication is getting easier, identity

606   proofing is getting harder as attackers have caught up to

607   first-generation solutions like static KBA.

608   This might actually be the most impactful area where the

609   government can help, by allowing consumers to ask agencies that

610   already have their personal information and have validated it,

611   in many cases with an in-person process, to then vouch for them

612   for -- with other parties that they seek to do business with.

613   The Social Security Administration and State Department and

614   Motor Vehicles have the most to offer here, and this is actually

615   a concept that was embraced in the 2016 report from the bipartisan

616   Commission on Enhancing National cybersecurity.

617   Here, the federal government should work to develop a

618   framework of standards and rules to make sure this is done in a

619   secure privacy-enhancing way and look at funding work to get it

620   started.

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

31

621   Finally, technology can help solve the problem but better

622   standards will be needed for companies and agencies to apply it.

623   Further investments in government research and standards work can

624   go a long way toward making it easier for any party in the public

625   or private sector to implement stronger identity solutions.

626   I appreciate the opportunity to testify today and look

627   forward to answering your questions.

628   [The prepared statement of Mr. Grant follows:]

629

630   **********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.

631   Mr. Griffith. I thank the gentleman and now recognize Mr.

632   Mierzwinski for five 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.

33

633   STATEMENT OF MR. MIERZWINSKI

634

635   Mr. Mierzwinski. Thank you, Vice Chairman and

636   Representative Castor and members of the committee.

637   The Equifax breach was an epic fail in a lot of different

638   ways. I know that this full committee has held hearings on it.

639   Mr. Walden, the chairman of the full committee, used an

640   excellent line when he said, "I can't fix stupid," when he was

641   talking about Equifax's many problems.

642   I agree with the chairman on that but I want to point out

643   a few other points about Equifax that may not have been pointed

644   out in that hearing.

645   First of all, I think everybody sees them as a credit bureau,

646   and that is true -- they are one of the big three credit bureaus

647   that collect information and sell it for the purpose of employment

648   and credit and insurance decisions.

649   They are gatekeepers to our financial and economic

650   opportunity. So it's very important that they do a better job.

651   In fact, that's their only job is buying and selling data. So

652   you can't blame Target or even OPM the same way you can blame

653   Equifax for their many, many epic fails in that -- in that debacle.

654   But I want to point out also -- and the Federal Trade

655   Commission has issued several reports on this -- Equifax is not

656   only a credit bureau. It is a data broker, and data brokers,

657   unlike credit bureaus, are ubiquitous in society and they are

658   virtually unregulated and they buy and sell information every day

659   that's very similar to credit reports but unregulated. So we need

660   to take a look at the data broker system and figure out a way to

661   regulate it more closely.

662   Second, I think we need to go back to first principles. Mr.

663   Hunt referred to data maximization. The code of fair information

664   practices says data minimization should be a goal and the code

665   of fair information practices is embedded in a number of our laws,

666   including the U.S. Privacy Act of 1974.

667   So we can't just protect all information. We've got to start

668   collecting less information and keeping it for shorter periods

669   of time.

670   We have already heard from several witnesses and members of

671   the committee about the problem of SSNs as identifiers and

672   authenticators.

673   But I want to point out that our credit reporting system,

674   how we obtain credit in society, a bad guy doesn't try to get your

675   credit report. That's very hard to do.

676   A bad guy gets your Social Security number and goes to a

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

35

677   creditor, and a creditor, being a trusted partner to the credit

678   bureaus, gets your credit report and gives credit to the imposter.

679   That's a very flawed system that needs to be fixed.

680   The principal thing that I think Congress should do in

681   response to Equifax, and I think it's bipartisan, is make credit

682   freezes free.

683   Credit freezes are the best way to protect your identify from

684   financial identity theft. But, unfortunately, they cost money

685   in most states.

686   The problem of KBA authentication has already been

687   discussed. I want to point out it's so obsolete it's pathetic

688   and it also upset -- it's not only bad because imposters can do

689   one-second searches on the internet and obtain answers to the

690   questions.

691   Sometimes consumers don't know the answers to the questions.

692   My colleague was asked how much credit her -- you know, her family

693   member Chester had. Chester was her dog. He died years ago.

694   She was five years old. Why is Chester a security question? What

695   is the name of your first student loan company? Was it Sallie

696   Mae or was it Navient? They keep changing the names of all of

697   these companies. It's all ludicrous.

698   On multi factor identification, I think it's a real positive

699   step. But I do want to point out that biometrics, the third

700   general multi factor authentication -- something you know,

701   something you have, and something you are -- privacy groups are

702   very concerned about databases of biometric information posing

703   privacy and civil liberties threats.

704   But on the other hand, if my fingerprint is only stored in

705   my phone, perhaps that's a better solution. I'm very encouraged

706   by the work that the other witnesses have talked about.

707   The FIDO Alliance and the NIST program have been open source

708   open standard multi stakeholder investigations of how to improve

709   our privacy and authentication mechanisms.

710   On the other hand, I contrast that to the credit card PCS

711   standards that have been imposed on merchants. The Target and

712   the Home Depot, the Michael's, et cetera -- all the merchant

713   breaches -- you can't blame the merchants for having to use an

714   obsolete credit card with a magnetic stripe.

715   And now the -- now the first have gone to a chip card, which

716   is a type of tokenization, and that is good but they could have

717   gone further. They could have gone to chip and PIN. They could

718   have gone to best available technology.

719   So we have made some progress but a lot more needs to be done.

720   Thank you very much for the time.

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

721   [The prepared statement of Mr. Mierzwinski follows:]

722

723   **********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.

724   Mr. Griffith. Thank you. Appreciate that, and we will now

725   begin the questioning and I will start with questions.

726   Mr. Hunt, in your testimony you talk about the exposure of

727   data due to accidental misconfigurations of cloud services. You

728   were certainly spot on.

729   One such misconfiguration was discovered in the federal

730   government this week and it has been reported that this is the

731   fifth time the government has suffered a similar accidental

732   exposure this year.

733   Indeed, many companies, including Uber, have suffered

734   information compromises because of these kinds of

735   misconfigurations.

736   Why does this keep happening? Is it really that easy to

737   accidentally share your cloud services with the world?

738   Mr. Hunt. Well, the easy answer to the last question is yes,

739   it is that easy. It's very often just a simple misconfiguration,

740   and the difference between, let's say, a storage account within

741   Amazon being protected and needed credentials in order to access

742   it and being wide open is literally one configuration that can

743   take seconds to make.

744   So in terms of why it's that easy or how come this keeps

745   happening so frequently, very often this is a competency problem.

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

746 So people have access to resources such as cloud services that

747 aren't sufficiently skilled in order to figure out how to

748 configure them securely. Sometimes it can just be a simple

749 oversight and there's not enough backup controls to identify when

750 something like this is exposed publicly.

751   It is also very difficult for organizations because when

752 cloud services are used they tend to very frequently sit outside

753 their known address base.

754   So, traditionally, an organization could say these are our

755 IP addresses, this is the range of our scope of assets and then

756 you can go onto the cloud and you can put things in totally outside

757 that construct.

758   And then compounding that as well we have this -- this, I

759 guess, construct called Shadow IT and for the longest time we have

760 had the concern of Shadow IT -- people working outside the formal

761 constructs of the way the IT department and organization should

762 run.

763   And today, it is very simple for someone in an organization

764 to go to the likes of Amazon and say, look, I would like a storage

765 account -- I am going to publish data there, and the IT department

766 never even knows about it.

767   So there's a number of factors leading to the prevalence of

768   what is now becoming a very common event.

769   Mr. Griffith. Now, are any of the data breaches included

770   in your service from such a misconfiguration?

771   Mr. Hunt. From which, sir?

772   Mr. Griffith. From -- from your service.

773   Mr. Hunt. Oh, from misconfiguration?

774   Mr. Griffith. Yes.

775   Mr. Hunt. Yes, many of them. So we are seeing many

776   incidents. The perfect example that comes to mind, earlier this

777   year we had an OIT device called a CloudPet.

778   It is literally a teddy bear with a listening device that

779   talks to the internet. Their data was left publicly exposed in

780   a database facing the worldwide web without a password. And,

781   again, that is just a simple misconfiguration on their behalf.

782   Mr. Griffith. Wow. What can companies do to decrease the

783   likelihood of this kind of a misconfiguration?

784   Mr. Hunt. It's a combination of things. To me, many of

785   these incidents, whether it be misconfiguration or flaws in

786   software, come back to education, and this is the sort of thing

787   we are trying to do with Pluralsight.

788   Let's try and get education out there to the people that are

789   building these systems and standing them up. Because so

790   frequently it is just such a simple little thing and had the person

791   understood what the ramifications of the configuration change

792   they're making or the code change they're making was, it wouldn't

793   have happened. So I would love to see more education.

794   Mr. Griffith. And what are the consequences? I mean, we

795   can all think of some. But what are the consequences of companies

796   exposing this kind of data?

797   Mr. Hunt. Really depends on the data. I mean, at the --

798   at the sort of the least end of the scale very often we are seeing

799   large amounts of email addresses and passwords.

800   Now, that then often becomes a skeleton key into other things

801   because we know that people reuse their passwords.

802   So that -- I almost hesitate to say that's the best that could

803   happen. But when we think about the worst that could happen,

804   well, now we start to talk about large amounts of very personal

805   data.

806   So we have been speaking about the impact of things like the

807   Equifax incident. South Africa just recently had an incident

808   which was data exposed as a backup on a publicly-facing server

809   that had information about the entire country and this included

810   their national identifier, so think about a Social Security

811   number, which within there also includes date of birth and gender,

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

42

812   and now we have got a whole country saying we literally had all

813   of its data published on the internet and we know that it had been

814   obtained by other unauthorized parties and redistributed.

815   But what do we do? And to me, that's sort of the worst case

816   scenario because now you got a whole country saying, how are we

817   going to do knowledge-based authentication when the knowledge

818   about the whole country has gone public?

819   Mr. Griffith. Now, from what I understand, when folks go

820   back and analyse many security instances like data breaches, they

821   find that somewhere along the line someone in the organization

822   chose convenience such as the ability to check their personal

823   email from their work computer, for example, over security. Have

824   you found that to be true as well, in your work?

825   Mr. Hunt. Absolutely. I mean, the concern with

826   convenience -- I will give you a really good analogy -- is very

827   often I will say to people, look, we might see an application

828   talking to a database that has effectively server admin rights

829   -- the most privileged user you could possibly have -- and I will

830   say to people, why would that happen. And they say, well, it was

831   easy -- it was much easier to give access to everything than to

832   start implementing fine-grained permissions. And they are

833   right, it is much easier. But that then leads to the problems

834   we have got here.

835   Mr. Griffith. And, sir, how do we make it easier to protect

836   things -- protect that data?

837   Mr. Hunt. Well, again, I go back to that education side.

838   This is people making mistakes unknowingly, and when we see these

839   happen over and over again and we look at the behaviors of the

840   individuals, very often it is because they've never been taught

841   what are the ramifications of setting this configuration or

842   writing code that way.

843   Mr. Griffith. Yes. I do think we all choose convenience

844   from time to time when we know in our hearts we ought not.

845   With that, I have to yield back because my time is up and

846   now recognize Ms. Castor of Florida for five minutes of questions.

847   Ms. Castor. Well, thank you, Mr. Chairman.

848   As the Equifax breach made all too clear, there's an

849   astounding amount of data that is collected by companies and

850   especially credit bureaus.

851   The Equifax breach, for example, exposed the personal

852   information including names, Social Security numbers, birth

853   dates, addresses, other sensitive data of almost 150 million

854   Americans.

855   Mr. Grant, if this data is out there, should companies no

856   longer use this information as a component of identity

857   verification online?

858   Mr. Grant. I wouldn't say that they shouldn't use the

859   information anymore but they should be smart about the ways in

860   which they use it and I think there needs to be a recognition,

861   you know, across government and industry that these

862   first-generation systems that we were using the attackers have

863   caught up with them.

864   So let's figure out where it can be valuable in a process

865   to establish identity or authenticate identity and where it can't

866   be. I think there are still tools that are out there that are

867   using some of this data that could be -- you know, I often talk

868   about, you know, you have an arrow with multiple quivers in terms

869   of, you know, the tools that you're using.

870   There still may be some value. But I think we need to

871   recognize that it is been greatly diminished and we need to focus

872   on next-generation solutions.

873   Ms. Castor. So, Mr. Mierzwinski, a similar question. In

874   your testimony, you stated in reference to Social Security numbers

875   that, quote, "you cannot authenticate with a number that is also

876   an identifier," especially one that anyone can obtain, thanks to

877   the data breach world that we live 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.

45

878   This seems like a good reason to prevent companies from using

879   the Social Security number as an authenticator. Is that right?

880   Mr. Mierzwinski. Well, I think you're absolutely right,

881   Congresswoman, and many people don't know that the Social Security

882   number was invented so long ago it doesn't even have a correct

883   check sum number.

884   When you type your credit card number and make a mistake in

885   an online form, it knows instantly. Your Social Security number

886   can be completely garbled and it wouldn't know.

887   The first five digits actually aren't really about you.

888   They're about when you were born and where you got your number

889   more than unique. So it is a very big mistake.

890   I am encouraged that some of my banks know that when I've

891   logged on from a new machine or even a new place. But others of

892   my banks and other companies that I do business with don't ask

893   me extra questions or don't want to send me a text.

894   So it is uneven how companies are doing better authentication

895   and, to me, you have also got to penalize them when they make a

896   mistake.

897   I realize Equifax and other firms will be penalized by the

898   market. However, I wonder whether regulators need more authority

899   to penalize companies that lose our info.

900   Ms. Castor. So let's talk about that especially. You

901   mentioned the data brokers. Even outside of data breaches,

902   internet-connected datasets contained vast information.

903   A University of North Carolina study showed that data brokers

904   can obtain almost anything from demographic data to financial data

905   to travel data.

906   In your opinion, are there adequate safeguards in place to

907   limit what information data brokers collect, store, and sell about

908   us? It seemed in your testimony you said no, it is kind of the

909   --

910   Mr. Mierzwinski. No, despite -- and you can find many items

911   on the record from me criticizing the credit bureaus and the Fair

912   Credit Reporting Act for being too weak. It actually is one of

913   our stronger privacy laws. There are virtually no laws that apply

914   to data brokers and they are out there in a Wild West ecosystem

915   of digital collection and selling of information about consumers

916   in real time, and as I believe the vice chairman pointed out in

917   his opening statement, a lot more information is being collected

918   into their databases.

919   Your locational information is, for one, a new piece that

920   should be protected that isn't protected under many laws.

921   Ms. Castor. So are there any incentives currently in place

922 for companies to minimize the data they collect and store?

923   Mr. Mierzwinski. Unfortunately, I don't know that there are

924 enough and there -- public shaming helps but regulatory

925 accountability would help even more, and companies just feel that

926 we are not their customers.

927   Consumers are not Equifax's customer. Mr. Smith, the

928 ex-CEO, said that before numerous committees over the last month.

929 Business is their customer. We are their product. We need to

930 get them to think about taking care of us, and they haven't.

931   Ms. Castor. Mr. Grant, thank you for all of your work on

932 the National Strategy for Trusted Identities. The identity

933 ecosystem adheres to fair information practice principles, one

934 of which is data minimization.

935   This is the idea that organizations should collect only

936 information that is directly relevant and necessary to accomplish

937 the specified purpose. Is that right?

938   Mr. Grant. Yes.

939   Ms. Castor. So now it seemed to me, in this day and age,

940 companies want to know everything about you. I am going to ask

941 you the same question. What incentives are currently in place

942 for companies to minimize the data they collect and store?

943   Mr. Grant. Well, I will say concerns both about regulatory

944 enforcement as well as liability that they might face by having

945 too much data.

946   You know, Mr. Hunt talked before about data maximization.

947 When I was running the NSTIC program there was a term one of our

948 staffers coined, which was data promiscuity -- the practice that,

949 you know, companies are just quite open in terms of collecting

950 and sharing gobs of data.

951   And I do think one thing you're starting to see now,

952 particularly when some of that data is exposed in a massive breach,

953 is other companies take a look at it and say, do we actually want

954 to have all of this data.

955   And so, you know, now that I am in the private sector I spend

956 a lot of time working with companies, advising companies on how

957 to minimize their risk, and I would say there are some companies

958 that still want to hoard data and there are some that are realizing

959 that it might be a liability and are actually trying to put

960 proactive measures in place to reduce the footprint of data that

961 they have on their customers and really focus only on what they

962 need.

963   So I do think a mix of regulation and liability does have

964 an impact in the marketplace. You know, certainly, if you look

965 across the ocean to what's happening in Europe right now with the

966 impending implementation of Europe's general data protection

967 regulation -- GDPR -- there's a lot of companies here in the U.S.

968 that are still going to be impacted by that and that's also causing

969 some firms to wake up and reevaluate in some cases what data they

970 collect, how they store it, how they use it.

971   Ms. Castor. Thank you.

972   Mr. Griffith. I thank the gentlelady for yielding back.

973   Now recognize the gentleman from New York, Mr. Collins, for

974 five minutes of questions.

975   Mr. Collins. Thank you, Mr. Chairman.

976   And Mr. Hunt, I guess it is 3:00 a.m. right now so I am hoping

977 you got some sleep on the flight coming up from Down Under.

978   I want to try to put today's hearing maybe in context just

979 for the everyday person. So many of us -- you know, every three

980 months one of our credit cards is accessed in some way. Usually

981 we find out because we get a notification -- a fraud alert from

982 American Express or Master Card. They've actually got some

983 algorithm somewhere that says, this looks unusual, or something.

984   So I want to make sure I understand. That's a little --

985 people doing that, grabbing our credit report and stealing our

986 numbers is perhaps different than the data breach area, or not?

987   Mr. Hunt. Where it probably differs to credit cards is there

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

988   are a lot of different places where credit cards are exposed which

989   may not be as a result of a data breach.

990   I've had my wife's card compromised several different times

991   now and, as you say, you hear from American Express --

992   Mr. Collins. Because I am sure she uses it daily.

993   [Laughter.]

994   Mr. Hunt. Well, she does appear to use it regularly,

995   evidently. When this happens, she will, as you say, get fraud

996   alerts from the bank.

997   Now, that could have been anything from -- we might have been

998   in a taxi in a particular location and they scribbled down the

999   number when they had physical access to it. You give it to someone

1000   at a restaurant -- that guy behind the counter. It could have

1001   happened in an incident like that. It could have been that a

1002   single merchant resold the data after purchasing something

1003   online.

1004   Now, that's not necessarily the same as someone who was a

1005   malicious party came along, found a vulnerability in software,

1006   and sucked out a million different records in one go.

1007   Mr. Collins. Yes. So I wanted to kind of make -- because

1008   I think sometimes we confuse the two and I think most of us are

1009   impacted by somebody grabbing our credit card more than not.

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

1010   Then we got to go to the inconvenience -- getting a new card,

1011 set up on autopay. You know, I probably have to do that three,

1012 four times a year even.

1013   So here we are talking about data breach. So now it begs

1014 the question, when someone is getting that, and I certainly

1015 understand someone, if they had enough, could try to apply for,

1016 I don't know, a mortgage, a something.

1017   But that probably doesn't impact too many Americans as much

1018 as somebody stealing their credit cards.

1019   So it kind of begs the question, these data brokers, as we

1020 call them -- it sounds like a business because there's guys --

1021 and it sounds like they're -- are they continuing to try to fill

1022 out, you know, for, you know, myself, you know, there's people

1023 with my same name, so I don't know.

1024   Are they sorting by my last name? My first name? My middle

1025 initial? As they find out that I, you know, just went to the SPCA

1026 and got a new cat, you know, what's the cat's name.

1027   You know, how are they sorting this? By Social Security

1028 number? By address, in multiple ways, and as you said, trading

1029 baseball cards -- are they doing this for fun? And then once they

1030 have it, and they're just out there selling it, why can't we catch

1031 these guys?

52

1032   If somebody -- I think of Raymond Reddington on "The Black

1033   List," you know. He'd be the guy buying this stuff. Why can't

1034   we find them, shut them down? And so that kind of general

1035   questions. What would you add to that?

1036   Mr. Hunt. I would say one point to maybe sort of

1037   disambiguify here is when I made the comment about trading

1038   baseball cards what I am talking about is there are a lot of

1039   individuals out there who obtain access to data breaches and then

1040   they redistribute them between peers -- not necessarily

1041   commercial legal entities like data brokers such as Equifax but

1042   individuals, in many cases children, sitting in their bedroom

1043   going, hey, I've got a data breach -- you have got this one --

1044   let's swap and we'll build up these personal collections.

1045   Now, that is not necessarily with malicious intent but it

1046   does lead to the redistribution and the growth of the amount of

1047   data that's out there.

1048   And then in terms of the data brokers, in terms of the legally

1049   operating entities, very often they refer to data enrichment,

1050   which is like let's just get as much data as we can about the

1051   individuals, refine it so that we have very, very clear pictures

1052   because that makes the product that they offer that much more

1053   valuable.

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

1054   And then whether they saw it by your Social Security number

1055   or your name or your job title, whatever it may be, that got

1056   significant amounts of data that they can offer people, whatever

1057   sort of sorting or filtering mechanism they like.

1058   Mr. Collins. So in this case, you're referring to a data

1059   broker as a legal entity --

1060   Mr. Hunt. Correct.

1061   Mr. Collins.   -- not a blacklister that's out there selling

1062   it?

1063   Mr. Hunt. That's right.

1064   Mr. Collins. All right. So the folks that are out there

1065   selling it on the darknet or whatever, just walk us through --

1066   we don't have a lot of time -- how are they finding their customers,

1067   verifying it is not an FBI or somebody under cover?

1068   Mr. Hunt. Well, they don't always get that right.

1069   [Laughter.]

1070   So how are they selling it? Well, very often we see data

1071   breaches being traded on the same sorts of marketplaces that are

1072   trading things like drugs.

1073   So we have seeing very prominent darkweb websites -- the Silk

1074   Road, Hansa Market, AlphaBay. Now, many of those services have

1075   now been shut down but others have emerged in their place and 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.

54

1076   operate on Tor hidden services on the darkweb, which does make

1077   it very difficult many times to actually track them down. So they

1078   operate illegal marketplaces and data breaches are another

1079   commodity like heroin.

1080   Mr. Collins. Well, I appreciate all your comments. My time

1081   is up. I yield back, and thank you for coming up from Australia.

1082   Mr. Griffith. I thank the gentleman for yielding back.

1083   I now recognize Mr. Tonko of New York for five minutes for

1084   questions.

1085   Mr. Tonko. Thank you, Mr. Chair.

1086   In recent years, as breaches have become more common,

1087   companies and technology have not kept pace to protect consumers.

1088   As more breaches occur, more consumers are at risk for identity

1089   theft and other crimes.

1090   While progress has been made, we must do much more to,

1091   obviously, protect consumers. Many ongoing concerns were

1092   brought to the forefront once again with the Equifax breach. More

1093   than 8 million New Yorkers were affected by the Equifax breach

1094   including many of my constituents.

1095   One constituent, who I will label as Lee from Albany, asked

1096   Equifax, why are you using this gross misconduct to turn your

1097   victims into customers for a paid monitoring service that you will

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

55

1098   profit from.

1099   Mr. Mierzwinski, can you speak to Lee's concerns that

1100   companies are profiting off these breaches?

1101   Mr. Mierzwinski. We think it is outrageous and we wish it

1102   would stop. The companies have turned consumers into cash cows.

1103   They're responsible for keeping our information safe and

1104   keeping it accurate. They don't, and so instead they say, you

1105   better buy this credit monitoring service at $19.95 a month, and

1106   the marketing of these services is extremely deceptive. Several

1107   banks have been fined by the bureau and several of the credit

1108   bureaus have been fined by the FTC.

1109   A third party company, Lifelock, has been fined by the FTC

1110   and numerous state attorneys general. After it violated the

1111   terms of its settlement order, it was fined an additional $100

1112   million for contempt.

1113   So the marketing of credit monitoring is unfair, and you

1114   don't need credit monitoring either because you can get your

1115   credit report for free under federal law. In seven states, you

1116   can get a second credit report for free from each of the three

1117   companies.

1118   If you file a fraud alert -- a 90-day fraud alert -- after

1119   you have been a victim of a breach, you could get an additional

1120 free credit report, get them every three months, and you have got

1121 your own free credit monitoring.

1122   But Equifax should not be profiting. We'd like to put a stop

1123 to it and we'd like them to not charge consumers for freezing.

1124   Mr. Tonko. Thank you.

1125   And Mr. Mierzwinski, again, you discussed the privacy risks

1126 that come along with biometrics. Can you elaborate on these

1127 risks?

1128   Mr. Mierzwinski. Well, very simply, I think that as we put

1129 our biometric information into databases, it becomes another

1130 commodity in the cloud.

1131   It becomes another way that you can steal information about

1132 a consumer, if you steal my fingerprints or my retina scan, it's

1133 -- you could clone yourself as me in a lot of different ways.

1134   I am not an expert on whether that is being done yet today,

1135 but we are very concerned and also concerned about the civil

1136 liberties aspects of government agencies getting access to the

1137 information in the databases without warrants, et cetera.

1138   Mr. Tonko. Mm-hmm. I thank you for that.

1139   And a 2017 New York Times article described the nightmare

1140 that Americans face when confronted with identity theft. The

1141 article referenced a study on identity theft and pointed out that,

1142 and I quote, "Last year, 15.4 million American victims of identity

1143 theft lost $16 billion."

1144 The article continues, describing cases where Americans were

1145 denied the ability to refinance their mortgages or tax refunds

1146 were fraudulently sent to hackers and other similar cases.

1147 So Mr. Mierzwinski, many companies use certain information

1148 to verify someone's identity like a full name, home address, and

1149 Social Security number. Now with the data for nearly half of

1150 Americans stolen, is it true that malicious actors could retrieve

1151 those identifiers?

1152 Mr. Mierzwinski. Absolutely malicious actors can retrieve

1153 your information in a variety of ways. They can even retrieve

1154 more information if they've only obtained some.

1155 So the Yahoo breach largely obtained for the bad guys phone

1156 numbers and email addresses. That's the way that you can then

1157 conduct phishing and spear phishing exploits to get more

1158 information from consumers or even call them on the phone and say,

1159 "I've got your Social Security number. I am going to read part

1160 of it to you. You read the rest of it to me" -- those kinds of

1161 gimmicks -- social engineering. It is easier than hacking,

1162 actually.

1163 Mr. Tonko. Mm-hmm. The article also makes the case 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.

58

1164 we shouldn't necessarily get rid of using Social Security numbers

1165 to identify someone but that we should stop using it as an

1166 authenticating factor.

1167   Mr. Grant, do you agree with that?

1168   Mr. Grant. Yes. I wrote an op-ed that was published in The

1169 Hill about a month ago that made that same point. I think we need

1170 to understand how Social Security numbers are both an identifier

1171 and an authenticator and essentially stop recognizing them for

1172 use of the latter. If I call my credit card company and they ask

1173 for the last four of my Social Security number, my answer should

1174 be, "Why in the world would you think that me knowing that actually

1175 proves that I am me?" My information has been stolen several times

1176 over. It could be anybody who's calling in making that claim.

1177   But as an identifier, look, identifiers are needed in the

1178 modern economy. The government needs a way to track how much

1179 money I am making from both my job and my bank accounts. You know,

1180 individual companies need an identifier as well.

1181   Let's just treat it as something that's widely available and

1182 I think once we acknowledge that it is not something that is a

1183 secret, then we can start to focus on what comes next, which are

1184 better solutions for identity verification, better solutions for

1185 authentication that don't have the weaknesses that the ones that

1186   we are using today have.

1187   Mr. Tonko. Thank you.

1188   And with that, I yield back, Mr. Chair.

1189   Mr. Griffith. I thank the gentleman, and now recognize Mr.

1190   Costello of Pennsylvania for five minutes for questioning.

1191   Mr. Costello. Thank you, Mr. Chairman. I am going to try

1192   this with my voice.

1193   To all three of you, I am just going to read through a series

1194   of questions and ask that you weigh in as appropriate.

1195   You talked -- you spoke in your testimony about the role of

1196   Social Security numbers both as they are used now and as they

1197   should be used in the future.

1198   In particular, you're both adamant about the need that we

1199   don't need to replace Social Security numbers as some have

1200   suggested we need to.

1201   Instead, you have said that using them or the need to change

1202   them from using them as identifiers and authenticators to using

1203   them solely as identifiers.

1204   My questions are oriented in this fashion. Are there

1205   barriers to moving away from Social Security numbers as both

1206   identifiers and authenticators? For example, are there

1207   government regulations that require them in certain instances?

1208   Are there private sector standards that recommend or require

1209   their collection? And how will these organizations begin making

1210   the change you suggested?

1211   How expensive both in terms of time and resources would this

1212   change be and are there any potential down sides, and if so, what

1213   are they?

1214   Mr. Grant. So I am happy to jump in with that first.

1215   I think one point you raised is there are a lot of entities

1216   that are required to collect my Social Security number.

1217   I started a new job at Venable five months ago. They needed

1218   to know my SSN. Any bank account that I open they need to know

1219   my SSN. And that's for the purpose of an identifier and I don't

1220   know that there are any real issues there with them continuing

1221   to use that.

1222   There are issues that are out there in terms of, you know,

1223   particularly when opening financial accounts. I mean, one big

1224   problem we have in this country is what, you know, many people

1225   refer to as synthetic identity fraud -- when you'll see fraudsters

1226   try and combine a real name and a real Social Security number that

1227   don't match and then start throwing it into the system in an

1228   attempt to establish credit, and that's, you know, one way that,

1229   you know, organizations are then defrauded or people are

1230   defrauded.

1231   I mean, so, you know, I think there's good reasons to keep

1232   using the SSN as an identifier but we could also use better systems

1233   to verify.

1234   One of the things I talked about in my opening statement was

1235   what government could actually do as a provider of identity

1236   verification services themselves.

1237   The Social Security Administration knows that there's a

1238   Jeremy Grant that has my Social Security number that matches but

1239   if I go to open a new account at a bank today or a mobile network

1240   operator or anybody else who's collecting it, there's no way to

1241   electronically verify that with Social Security that that really

1242   matches up.

1243   There's a paper-based system that requires a wet signature.

1244   It was a great thing 20 years ago. It is 2017 now. I think you

1245   could actually help cut down on fraud in new account opening if

1246   there was an electronic way for Social Security to validate those

1247   numbers if queried.

1248   I think where there's going to be bigger issues -- you were

1249   asking about barriers and costs and things like that -- is where

1250   we replace the Social Security numbers and authenticator.

1251   So I can make fun of the credit card company I called last

1252 week who asked for the last four of my Social Security number and,

1253 obviously, there's no security value to that in 2017.

1254 But their next question is, well, then how do I authenticate

1255 you when I am talking to you on the phone, and that's a much harder

1256 question. I think there's some interesting products. There's

1257 new standards that are emerging. There's -- there are ways that

1258 you can do it. But there tends to be -- the pace of adoption tends

1259 to lag the creation of new technology.

1260 And so I think this is actually an area where I would love

1261 to see government partnering with industry focus more is how can

1262 we identify where those are -- where there are promising

1263 technologies that could replace the first-generation tools that

1264 have, you know, started to fail and accelerate the pace of adoption

1265 everyplace.

1266 Mr. Mierzwinski. I agree.

1267 Mr. Costello. That's a good answer.

1268 Mr. Mierzwinski. Yes. Try to keep some of your time for

1269 you.

1270 Mr. Costello. Very good. I will yield back, Mr. Chair.

1271 Mr. Griffith. I thank the gentleman for yielding back.

1272 I now recognize Ms. Clarke of New York for five minutes for

1273 questions.

1274   Ms. Clarke. I thank you, Mr. Chairman. I thank our ranking

1275   member. I thank our panellists for their expert testimony here

1276   today.

1277   And I wanted to bring up the national strategy for trusted

1278   identities in cyberspace. Under President Obama, the White House

1279   released this strategy and this spurred the public and private

1280   sectors to collaborate on issues related to identities and online

1281   transactions.

1282   Mr. Grant, is it accurate that this strategy laid the

1283   framework for privacy-enhancing technology as well as identity

1284   solutions that must be secure and cost effective?

1285   Mr. Grant. Well, I would say it helped. I think where NSTIC

1286   really helped was throwing down a marker in 2011 for an industry

1287   that, you know, hadn't really started to think about this yet,

1288   and when I look at the impact several years later, you know --

1289   I talked about this in my written statement -- companies that liked

1290   it came in and said, hey, this is a great idea -- how can we actually

1291   work with you to come up with solutions that align with it.

1292   Even companies that didn't like the fact that the government

1293   had thrown down a marker still had to pay attention to it because

1294   their customers were focussing on it.

1295   So when I look at where the market is today, look, we still

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

64

1296   have plenty of problems in the identity space. We wouldn't be

1297   having this hearing if it wasn't the case. But I think the

1298   strategy helped and some of the specific activities that we --

1299   that we sponsored and funded out of NIST during the time that there

1300   was a national program office implementing NSTIC really helped

1301   to move the market along at a point much faster than it would have

1302   gone otherwise and, you know, also pointed the way to, you know,

1303   create the -- you know, just pointing out basic things like

1304   security doesn't have to be at odds with privacy.

1305   Security doesn't have to be at odds with user experience.

1306   Those are concepts -- it is not a radical statement to make but

1307   there were some vendors in the space who seemed to think that they

1308   were going to be at odds and this helped -- helped to show that

1309   there could be other ways.

1310   Ms. Clarke. So what -- can you elaborate a little bit more

1311   as to what a privacy-enhancing solution may look like in the age

1312   of data breaches?

1313   Mr. Grant. Sure. So, you know, the concept of privacy

1314   enhancing it is, you know, how does -- how do you create solutions

1315   that can actually give people more control over their personal

1316   information -- have more choice in terms of what attributes they

1317   choose to share about themselves when they go online.

1318   And, you know, it is a catch-all term. But in terms of

1319 practical application, I think it is, you know, something you see

1320 today. Let's say you're logging in to a website with a social

1321 provider and they now give you radio buttons that, you know, let

1322 you choose -- do I just share my name?

1323   Do I log in anonymously or do I share -- let's say it is using

1324 Facebook Connect -- a whole bunch of information about me with

1325 that site. That's, you know, one example of giving consumers

1326 choice in a way that's also pretty easy to select, you know, with

1327 radio buttons, for example, that you can click on or off. That

1328 is something that we didn't have in the marketplace before.

1329   I think there's other interesting approaches. You know,

1330 people can get -- we could really go down the rabbit hole in terms

1331 of talking about privacy-enhancing encryption, which is an area

1332 that I will say there's been a ton of R&D done but I would say

1333 we still have barriers in the marketplace in terms of coming up

1334 with systems that can scale.

1335   I know there's really a commercial -- a need for. We, you

1336 know, funded a lot of research there as well and NIST continues

1337 to do good work there today. That's probably some of the next

1338 generation work, I think, in terms of where the market focus is

1339 next.

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

1340   Ms. Clarke. So can you tell us the benefits of a universal

1341 two-factor authentication or similar types of technologies that

1342 secure a user's identity?

1343   Mr. Grant. Well, it is a universal two factor. Whether it

1344 is universal or whether you're just using two-factor

1345 authentication everywhere. You know, I mentioned in my opening

1346 statement 81 percent of breaches last year were caused by

1347 exploiting passwords.

1348   There is a reason for that. The password is really easy to

1349 compromise and the notion that there's such a thing as a secure

1350 password just doesn't make sense. You know, a lot of the attacks

1351 we see these days are speak phishing attacks where you get

1352 something that looks like a normal login to your email provider

1353 or your bank but it is not. It is somebody who's inside trying

1354 to phish your user name and password.

1355   If you have unphishable two-factor authentication behind it,

1356 that attack doesn't work anymore. Although one problem we are

1357 actually seeing in the marketplace is some of the first-generation

1358 tools that we have seen for two-factor authentication -- things

1359 like getting a code through SMS or, you know, through an app on

1360 your phone.

1361   That is phishable as well. And so, you know, I keep making

1362   the point we had solutions that were good for a while and now the

1363   attackers have caught up with them.

1364   Moving to unphishable authentication -- you know, we have

1365   talked in this hearing about, you know, standards bodies like the

1366   FIDO Alliance that are coming up with solutions based on public

1367   key crypto, which is unphishable. That, I think, is where, you

1368   know, we need to focus there.

1369   Ms. Clarke. Where we need to go. Okay.

1370   And just sort of in closing, you know, I am glad that we

1371   somewhat have a roadmap to improve the security of our online

1372   identities but it seems that more efforts are needed to implement

1373   these effective solutions and we need to continue to evolve, as

1374   you have stated, because we sort of get static after a while and,

1375   of course, there are those who are out there constantly working

1376   at how to phish and break through.

1377   So thank you for your response today. Hopefully, we will

1378   heed what you have shared with us today.

1379   I yield back, Mr. Chairman.

1380   Mr. Griffith. I thank the gentlelady for yielding back.

1381   I now recognize Mr. Walberg of Michigan for five minutes of

1382   questions.

1383   Mr. Walberg. Thank you, Mr. Chairman, and thanks to the

1384   panel for being here.

1385   Mr. Hunt, I appreciate you coming all that distance. In

1386   fact, I've often had some sinister thoughts of sending some of

1387   these hackers, et cetera, back to Darwin, Australia, and let them

1388   confront some of the wildlife there in that beautiful but

1389   dangerous part of your great country. But I won't suggest that.

1390   One of the reasons that we are having this hearing today is

1391   to shine a light on a problem that we think is getting worse,

1392   namely, that there is so much data available on individuals from

1393   these various breaches that malicious actors can package or enrich

1394   data to create very robust profiles of almost any given person.

1395   Is that something that you have seen or heard about and if

1396   so is it a growing problem?

1397   Mr. Hunt. Yes. Look, it is certainly a concerning thing

1398   because, obviously, the more personal attributes you can gather

1399   about an individual the richer the picture you have.

1400   And then when it then comes to things like knowledge-based

1401   authentication you start to build up many different attributes.

1402   And in my written testimony I talk about the concern of aggregating

1403   from multiple services, and they're not always data breaches

1404   either.

1405   So someone might take certain attributes from one data breach

1406   -- let's say a name and a birth date. They'll go to another data

1407   breach and they may get gender and home address.

1408   And then they'll go to open source intelligence sources such

1409   as LinkedIn, Facebook, Twitter, and aggregate further data

1410   attributes from there -- your profile photo, your social

1411   connections. And the real concern I have there is that even

1412   beyond just data breaches alone there are so many sources of

1413   information that we literally willing publish ourselves publicly

1414   that we now have to start to work on this assumption that so many

1415   known attributes about ourselves, which we did previously

1416   consider to be personal attributes, are now public and that's the

1417   concern I have. There's just so many different sources and it

1418   is not just data breaches.

1419   Mr. Walberg. And that's what makes it so valuable then, that

1420   --

1421   Mr. Hunt. Oh, absolutely, and I can see why the likes of

1422   legally operating data aggregators are running great businesses

1423   these days because there is so much data that they can obtain from

1424   us.

1425   Mr. Walberg. Yes.

1426   Mr. Grant, as former head of NSTIC, is -- this is likely an

1427   issue that you're familiar with as well. Did NSTIC look at this

1428 kind of problem and, if so, what were its conclusions and

1429 recommendations?

1430   Mr. Grant. So I would say we spend a lot of time looking

1431 at it in the Trusted Identities Group and NIST continues to focus

1432 on this.

1433   You know, I think probably the most -- well, there's a lot

1434 of things that NIST has done in this space that's been Impactful.

1435   But one that I would point to are the updated digital identity

1436 guidelines. One of the NIST special publications, 800-63-3, is

1437 the title or the code that was put out this past summer, which

1438 was an effort led by my old office to basically take a look at

1439 what is the modern state of solutions in terms of what we can use

1440 for identity verification and authentication in the marketplace

1441 and also recognize where some of the attackers have caught up with

1442 some of the old technologies.

1443   And so they published new guidance this past summer which

1444 I think -- you know, what's been nice about it is not just in

1445 government but also a number of entities in industry have looked

1446 at this and said, this is fantastic -- this is a guidebook that

1447 we can use as we are building solutions for the private sector

1448 to make sure that we are, you know, both taking into account new

1449 technologies and new standards that are emerging -- things like

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

71

1450   FIDO as well as make sure that we are not using some of the legacy

1451   solutions that just aren't as good anymore.

1452   So, you know, certainly, in the topic of identity

1453   verification, one of the things that the new guidelines did was

1454   diminish the role of KBA in terms of how much you can trust it

1455   for identity proofing.

1456   It establishes that there's still a role for it in the process

1457   of identity resolution, you know, trying to figure out whether

1458   I am the Jeremy Grant who's actually applying for an account but

1459   says you cannot use it alone for, you know, full-blown identity

1460   verification. That was a big change from what we've seen in the

1461   past.

1462   So, you know, one thing I mentioned in my written testimony

1463   some of the budget for NIST work in this area has been proposed

1464   for a cut in 2018 at a time when everybody's looking at, you know,

1465   where we can actually take some actions after events like the

1466   Equifax breach. I think we, you know, are going to continue to

1467   need more funding for research and standards in this area, both

1468   to help government implement better solutions as well as the

1469   private sector.

1470   Mr. Walberg. What updated standards are you talking about

1471   there?

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

72

1472   Mr. Grant. There is updated -- well, I think there's other

1473   work to be done still. So I think NIST has put out digital

1474   identity guidelines.

1475   I would say two things. One, attackers are always evolving

1476   and technology is always evolving and so it is something that

1477   should be updated I would say, you know, on a regular basis rather

1478   than, you know, a cycle that's every five or 10 years, which is

1479   often how NIST tackles the special publications.

1480   Beyond that, I think there's other research for areas. You

1481   know, for example, one of the questions that Mr. Hunt was asked

1482   before was about the security of cloud services and how entities

1483   are getting into that.

1484   And often, again, the attack vector there when you're

1485   guarding against big enterprise class data breaches is through

1486   identity.

1487   I think NIST could do a lot more work looking at enterprise

1488   identity and how you actually manage administration,

1489   authentication, authorization, analytics, and audit -- what I

1490   call the five A's of the identity life cycle.

1491   There is not great guidance out there anywhere in the world

1492   and NIST is really well poised to help enterprises apply better

1493   identity 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.

73

1494   Mr. Walberg. Thank you. My time has expired.

1495   I yield back.

1496   Mr. Griffith. I thank the gentleman for yielding back and

1497   now recognize Representative Jan Schakowsky of Illinois. The

1498   gentlelady is recognized for five minutes.

1499   Ms. Schakowsky. Thank you so much.

1500   As we talk about consumer protection, which has really kind

1501   of been my bailiwick for a very long time, I have to mention what's

1502   going on right now at the Consumer Financial Protection Bureau.

1503   OMB Director Mick Mulvaney is serving now as acting director

1504   as his appointment continues to be challenged in the -- in the

1505   courts and Mr. Mulvaney has been pretty much a longtime opponent

1506   of the CFPB and no friend of consumer protection regulations.

1507   He has already put a hiring freeze and a regulatory freeze

1508   in place at the agency. So Mr. Mierzwinski, I wondered if you

1509   could just share your thoughts on what is currently going on at

1510   the CFPB and perhaps how it relates now to this issue also of data

1511   protection, et cetera.

1512   Mr. Mierzwinski. Well, thank you, Congresswoman, and of

1513   course, the Consumer Bureau was created after the big collapse

1514   of the economy and it was designed to be independent of the

1515   political process that has corrupted a lot of the control of how

1516   we protect consumers in the financial system.

1517   By appointing -- by suggesting that the head of the OMB, a

1518   deeply political agency of the White House, could also at the same

1519   time be the director of the independent Consumer Bureau, we just

1520   don't think that computes and we support Director Cordray's

1521   appointment of Leandra English as acting director.

1522   We truly recognize the president has the authority to

1523   eventually nominate and get someone confirmed by the Senate. But

1524   we hope that person is qualified as a consumer advocate and is

1525   not someone who has attacked the bureau and called it a sick, sad

1526   joke, as the current acting director has.

1527   The Consumer Bureau, in just six years of existence, has

1528   recovered over $12 billion -- about $12 billion for 29 million

1529   Americans and has restored confidence in the financial system.

1530   So we like -- we'd like to protect it. Going forward, you

1531   have pointed out one issue that is in conflict there is actually

1532   data security. Interestingly, the Consumer Bureau gained

1533   authority over Equifax when it sells credit reports through the

1534   Fair Credit Reporting Act.

1535   But the Gramm-Leach-Bliley Act under the Federal Trade

1536   Commission still controls on data security for a number of

1537   nonbanks including the credit bureaus. That's a real problem.

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

75

1538   Ms. Schakowsky. Yes, although before he left, Chairman

1539   Cordray said that he thought that there ought to be embedded

1540   regulators at Equifax and companies -- and the other companies.

1541   Mr. Mierzwinski. Well, actually, he does have the authority

1542   or he did have. The bureau still retains the authority to

1543   supervise Equifax in the same manner that bank regulators

1544   including the bureau supervise banks, meaning the ability to be

1545   there in an embedded basis and look for problems before they get

1546   bad and also to look at the toxic -- not the toxic but the secret

1547   sauce that the company uses to generate its credit scores.

1548   There are a lot of things that the bureau can and should do.

1549   But there is this one little piece of Gramm-Leach-Bliley that says

1550   the Federal Trade Commission is still the regulator for when you

1551   have a breach, when you have to notify.

1552   The Federal Trade Commission rule still has not created a

1553   notification standard at the federal level and this is something

1554   people may not be aware of. The Federal Trade Commission under

1555   Gramm-Leach-Bliley cannot impose a penalty for the first

1556   violation of the data security rules.

1557   The bureau can and any bank regulator can impose a penalty

1558   for any first violation by companies they regulate. The Federal

1559   Trade Commission cannot.

1560   Ms. Schakowsky. So regardless of how big the breach is,

1561   how many people are affected, they do not have the authority?

1562   Mr. Mierzwinski. Not under their statute and not under

1563   their regulations. They've never done it so I don't believe they

1564   have the authority and it is been confirmed to me by former staff

1565   there.

1566   Ms. Schakowsky. Oh, I see. Do I have time?

1567   Well, let me see if I can get to one last question and that

1568   is about credit freezes. So the long-term risk from data breaches

1569   underscores the need for strong data security and breach

1570   notification legislation such as the -- I have a bill called the

1571   Secure and Protect America's Data Act that I introduced with

1572   Ranking Member Pallone, several other members of this committee.

1573   So, again, Mr. Mierzwinski, when a company fails to protect

1574   consumers' data, then where does that leave the consumer? And

1575   let me just add also in the wake of the Equifax breach you have

1576   talked about making credit freezes free for consumers. How would

1577   that help?

1578   Mr. Mierzwinski. Well, how -- making credit freezes free

1579   would give us control of our own data, and by the way, that has

1580   almost become a bipartisan issue.

1581   The next step is to make credit freezes the default on switch.

1582   Make the consumer information always protected until the consumer

1583   agrees to turn it on.

1584   Ms. Schakowsky. So the --

1585   Mr. Mierzwinski. The opposite of the current situation.

1586   Ms. Schakowsky. Okay. Thank you so much. I yield back.

1587   Mr. Mierzwinski. Thank you.

1588   Mr. Griffith. Appreciate it. The gentlelady yields back.

1589   I now recognize the gentlelady from Indiana, Mrs. Brooks.

1590   Mrs. Brooks. Thank you, Mr. Chairman, and thank you to all

1591   of our witnesses for being here.

1592   I am a former federal prosecutor -- former U.S. attorney that

1593   worked on and prosecuted identity theft cases between 2001 and

1594   2007. So this is certainly not something new.

1595   I haven't heard very much, quite frankly though, about going

1596   after the bad guys, and we are talking about the hackers and I

1597   want to learn a little bit more.

1598   And Mr. Hunt, when you talked about the analogy of it is like

1599   shopping for heroin or so forth on the darknet and so forth, could

1600   you please talk with me a little bit more? Because I haven't been

1601   in that world, quite frankly, since '07 and really want to learn

1602   a little bit more about the buyers, the sellers, and how do they

1603   purchase it, select their buyers and sellers.

1604   Do they earn reputations on the darknet? Can you tell us

1605 a little bit, and then for yourself and maybe Mr. Grant a little

1606 bit about what kind of cooperation you have engaged in with law

1607 enforcement.

1608   Mr. Hunt?

1609   Mr. Hunt. I think we can sort of speak to the last part of

1610 the question first, which is around reputation, so how do people

1611 establish a reputation.

1612   One of the quite intriguing things when you do see these dark

1613 market marketplaces or darkweb marketplaces is that in many ways

1614 they look very familiar.

1615   They look like an eBay, for example, and there are buyers

1616 and sellers on there that have a reputation that they gain over

1617 a series of trades. Now, of course, the difference is they're

1618 not buying iPhones or consumer electronics. It is, literally,

1619 drugs, data breaches, and so on.

1620   So that's sort of the first part of the answer. The

1621 establish a reputation. In terms of then identifying who those

1622 parties are, one of the difficulties we have with privacy and

1623 anonymity tools is whilst they're very good for maintaining

1624 privacy and anonymity for people that want to do good things,

1625 they're also very good at maintaining privacy and anonymity for

1626   people doing bad things.

1627   Now, we have seen a number of these marketplaces taken down

1628   over time but, obviously, they are much harder to track down.

1629   I guess to the other points, one of the things that sort of

1630   concerns us is that there is a thriving marketplace for this data

1631   and there are, I guess, various shades of gray in terms of who

1632   finds this data attractive.

1633   That's, clearly, criminals -- those who literally want to

1634   go out and mount identity theft attacks. They find this data

1635   attractive.

1636   One of the things that worries me a little bit more is that

1637   it is also an attractive piece of information for more mainstream

1638   legitimate organizations who are looking to gain access to this

1639   data so that they can figure out which of their customers are

1640   protected.

1641   So we are now seeing very mainstream online web properties

1642   that many of us know and use on a daily basis that will tell people

1643   when they have appeared in a data breach and some of these are

1644   actually purchasing information in order to gain access to that

1645   to protect their customers.

1646   And, frankly, that -- I am a little bit torn with that because

1647   I understand the desire to protect their consumers but I also worry

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

1648   about the incentives that provides those who are breaking into

1649   systems.

1650   Mrs. Brooks. Mr. Grant, anything you want to add?

1651   Mr. Grant. Not too much. I mean, my -- look, law

1652   enforcement is quite important. It is -- I think as Mr. Hunt

1653   pointed out, it is becoming quite hard to attract people down in

1654   part because of the international nature of, you know, many of

1655   the criminal rings that are actually running all of these, you

1656   know, marketplaces and what not.

1657   I would agree in terms of what, you know, Mr. Hunt said as

1658   well in terms of the same tools that can protect us and keep us

1659   anonymous can also be protecting them. So there are definitely

1660   challenges there.

1661   Mrs. Brooks. Has there also been evidence that

1662   nation-states besides entities, individuals, criminal

1663   organizations are involved in this as well?

1664   Mr. Grant. Absolutely. I mean, that's something we

1665   haven't talked about much. I am sure most of us in this room were

1666   victims of the OPM breach, which I guess I appreciate that the

1667   government is giving me credit monitoring services for this.

1668   I don't think that the government of China is looking to

1669   establish credit in my name. They're interested in looking

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

81

1670   through the 75 pages or so of my SF-86 and figuring out if they

1671   can compromise me because I have a top secret clearance.

1672   But this is certainly something that has been quite

1673   interesting to other nation states who are looking to execute

1674   attacks, you know, both for those purposes as well as just for,

1675   you know, getting into basic accounts.

1676   Again, if we are protecting access to an account with only

1677   something like static KBA and they've now stolen the answers to

1678   those questions, well, then you can get into them and do things

1679   with them.

1680   You know, likewise, Mr. Mierzwinski talked before about, you

1681   know, some of the risks of biometrics. All of my fingerprints

1682   are now sitting in another country somewhere because of the OPM

1683   breach, which means I wouldn't feel particularly comfortable

1684   using anything that's doing remote match fingerprint to secure

1685   anything that I care about.

1686   That said, I am really comfortable with using a fingerprint

1687   on my phone because you have to come get my device out of my hands

1688   first before you can compromise it.

1689   Mrs. Brooks. Mr. Mierzwinski mentioned that the credit

1690   monitoring services maybe have been not very honest in their

1691   practices.

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

82

1692   Do you agree that when we receive these requests after we've

1693   been a target of a breach that people should or should not be

1694   accepting those services by the company?

1695   Mr. Grant.   You know, I don't think it hurts to accept them.

1696   Whether you pay for them is another question that I think --

1697   Mrs. Brooks.   Right.

1698   Mr. Grant.   -- you know, folks are asking right now.   Look,

1699   I think they are helpful because it is good to know if something

1700   is happening.   It is good to be able to monitor your account.

1701   Whether you need to pay for it is another question.   From,

1702   you know, the government perspective as a victim of the OPM breach

1703   I don't know what value it offers me other than it is nice thing

1704   to have to be able to keep close watch on my credit.

1705   So it -- you know, value in the service, yes.   Whether, you

1706   know, I want to pay for it as a consumer that's another question.

1707   Mrs. Brooks.   Thank you.   Thank you all for your work.

1708   Yield back.

1709   Mr. Griffith.   I now -- thank you.

1710   I know recognize the gentleman from Georgia, Mr. Carter, for

1711   five minutes of questioning.

1712   Mr. Carter.   Thank you, Mr. Chairman, and thank all of you

1713   for being here and for your efforts to get here.   Appreciate it

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

83

1714   very much.

1715   This is, obviously, very, very important to all of us. I

1716   want to start with you, Mr. Grant, and just ask you if you can,

1717   and please dumb it down for me, if you will, what are trust marks?

1718   Can you just explain that to me?

1719   Mr. Grant. Trust marks -- sure. Best example of a trust

1720   mark is the Visa logo that's on two credit cards in my wallet.

1721   So that if I go down to the cafeteria here afterwards and

1722   have lunch with Troy or Ed, the cafeteria doesn't really care which

1723   credit card I pay with. I got one issued by Capital One and one

1724   issued by Chase.

1725   Because it is got that Visa trust mark on it, which stands

1726   for a bunch of standards and operating rules that govern

1727   everything from how that card's authenticated at the point of sale

1728   terminal, what security is in place, how long it takes for my bank

1729   to pay the cafeteria for my lunch, what transaction rate that

1730   they're actually going to pay in terms of, you know, the fee for

1731   processing that, and some would argue most importantly if -- let's

1732   say Chairman -- Vice Chairman Griffith steals my credit card and

1733   buys lunch for the committee and I contest that with my bank, what

1734   am I liable for and what's the merchant liable for.

1735   So the trust mark is essentially something that represents

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

1736   all those standards and operating rules that in the credit card

1737   network everybody who's an issuing bank has to follow and

1738   everybody else has to follow.

1739   In the identity space, one argument -- this was a lot of the

1740   focus of NSTIC is that we need to create something similar to the

1741   Visa network before identity, which is that I could have the issuer

1742   be my state DMV or the Social Security Administration, my bank,

1743   my mobile network operator.

1744   It could be an advocacy group like the NRA or the ACLU or

1745   U.S. PIRG, who all could validate my identity a certain way, issue

1746   me a credential that I could use everywhere and the reason it would

1747   be trusted is because it has that trust mark.

1748   Mr. Carter. Well, that's really what I am getting at because

1749   as I understand it, the Trusted Identities Group has actually

1750   farmed out, if you will, pilot projects and the Georgia Tech

1751   Research Institute has actually come up with the emphasis on the

1752   machine-readable trust marks, and it is been very successful and

1753   the results have been positive, particularly when it was -- when

1754   it was over a trusted framework and that would encourage greater

1755   trust.

1756   How can this be implemented in industry? How can we use

1757   this?

1758   Mr. Grant. So I don't think -- you know, a little bit of

1759 background on the GTRI pilot that was one of the ones that I

1760 selected for funding when I was, you know, running the NSTIC

1761 program and the idea was, you know, how can you do something for

1762 identity that's, you know, similar to what you see in financial

1763 services.

1764   I would say, you know, where it has gone as a pilot, it was

1765 a great -- look, it is a pilot. It is a proof of concept,

1766 basically. It isn't something that's been picked up yet by

1767 industry.

1768   What I can say, though, is that work is being looked at by

1769 -- I don't want to break confidentiality with anybody I am, you

1770 know, doing work with now.

1771   Mr. Carter. Right. Right.

1772   Mr. Grant. But some bigger players that matter in the

1773 ecosystem who are actually looking at taking that similar concept

1774 and actually developing a, you know, broader federated identity

1775 system that could be led by the private sector for making it easier

1776 for consumers to identify themselves.

1777   The idea would be to basically leverage work that's being

1778 done there already with I can actually say some financial

1779 services.

1780   Since banks know you, thanks to the Know Your Customer rules

1781 that they go through and you might trust your bank -- not everybody

1782 does but some might -- how could they vouch for you other places

1783 when you're looking to open up a new account.

1784   Mr. Carter. Right. But do you agree that this is kind of

1785 the route we ought to be going?

1786   Mr. Grant. I think -- yes, I think it is a big part of the

1787 solution. I don't know that trust marks are going to solve

1788 everything. You know, look, so we did some good things with

1789 NSTIC.

1790   One of the things we didn't do is solve all the problems and

1791 it is because it is really complicated and there's a whole bunch

1792 of, you know, whether it is legal barriers, technical barriers,

1793 how do you create something that's really easy for consumers to

1794 use. There's issues that are out there.

1795   For as much as everybody loves to beat up on KBA and what

1796 the credit bureaus do, there's a reason it is been used so much

1797 in the market for years because that for many people it is work.

1798   Mr. Carter. Right.

1799   Mr. Grant. I am applying for a new credit card. I can do

1800 something instantly. When I went to lease a new car for my wife

1801 a year ago, I was able to get quick credit.

1802   So I don't want to suggest we throw the baby out with the

1803   bath water because there's problems. It is more realizing where

1804   attackers have caught up and how do we develop better solutions.

1805   Mr. Carter. Okay.

1806   Mr. Hunt, any -- any comments on trust marks and how it can

1807   be implemented into the private sector?

1808   Mr. Hunt. I think I would probably defer back to Mr. Grant

1809   as the expert on trust marks there.

1810   Mr. Carter. Right. Right.

1811   Were there any other new technologies that you find

1812   interesting and perhaps that have some potential?

1813   Mr. Hunt. I think ultimately we are going to see an

1814   augmentation of different practices. I mean, many people, for

1815   example, say, well look, is the answer biometrics or is the answer

1816   physical tokens.

1817   And where we are getting to now is I think an acknowledgement

1818   that we can't rely on one single knowledge-based authentication

1819   attribute, for example -- that we do have many other things

1820   available to us now that we didn't have, say, two, decades ago.

1821   We have ubiquitous mobile devices with internet

1822   connectivity. We have SMS. We have other forms of identifiers

1823   like physical YubiKey tokens, for example. And I think the right

1824   strategy moving forward is going to be the right augmentation of

1825   those under the right scenarios, depending on the trust level that

1826   you need to establish.

1827   Mr. Carter. Great. Thank you all again, and I yield back.

1828   Mr. Griffith. I thank the gentleman for yielding back. I

1829   do have a couple of follow-up questions just to try to clarify

1830   some things. Staff did a nice job, as they always do, in educating

1831   me beforehand. But, Mr. Grant, you used the term public encrypto.

1832   Mr. Grant. No, public key crypto.

1833   Mr. Griffith. Oh. And what does that mean?

1834   Mr. Grant. Well, so there's -- we can get really geeky

1835   talking about cryptography now -- there's essentially two ways

1836   you can manage cryptographic keys.

1837   One is called symmetric-key, which is when I got a key and

1838   you know the key, and I have to present the key to you for it to

1839   match. It is a lot -- similar to the way passwords work.

1840   The other is what's commonly known as asymmetric public key

1841   cryptography, or PKI for public key infrastructure. It is what

1842   the Defense Department as well as the federal government had been

1843   using for years, in many cases in lieu of passwords, in order to,

1844   you know, come up with unphishable authentication to protect

1845   federal networks and systems.

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

1846   At the end of the day, the concept is rather than each entity

1847 having the same key, I get a key pair, and the public key is known

1848 to everybody but the private key is only residing with me.

1849   It can be in my mobile phone. It could be in my computer.

1850 It can be on a device like the YubiKey, which is -- that Mr. Hunt

1851 mentioned which is a FIDO standard token, and when I am logging

1852 in someplace, I am basically asked to sign a cryptographic

1853 challenge where my public key is presented but the only way I can

1854 get in is if I have the corresponding private key with me

1855 physically.

1856   And so the -- we could really go into the details of it in

1857 ways that would make everybody's head explode. It is not -- this

1858 is actually one of the problems with -- about the adoption of

1859 technology, by the way.

1860   It has been very complicated. But I think the most important

1861 point to keep in mind is it is a way to deliver unphishable

1862 authentication. It is not based on shared secrets.

1863   And when I talk about how attackers have caught up not only

1864 to passwords but also things like SMS codes or other one-time

1865 passwords that are only good for 30 seconds, you know, that 30

1866 seconds is still enough for a moderately skilled attacker to phish

1867 my authentication code.

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

1868   Asymmetric public key crypto is where we should be building

1869   authentication solutions in the future so that we don't have

1870   phishable authentication.

1871   Mr. Griffith. All right. I appreciate that.

1872   Mr. Hunt, you travelled a long way. Is there anything that

1873   you had a burning desire to tell us that you haven't had an

1874   opportunity already to do so?

1875   Mr. Hunt. I think that the other thing I would add,

1876   obviously, I am very interested in how do we stem the flood of

1877   data breaches that we are seeing. And, you know, the things that

1878   really come to my mind that I would love to see implemented I

1879   mentioned education.

1880   So we are making lots of fundamental little mistakes.

1881   Another thing that's very important is making the disclosure of

1882   these incidents much easier.

1883   So I myself have been in this situation many times where

1884   someone has sent me data from an organization and just the ability

1885   to disclose it to the company, to find the right person who will

1886   listen, who will take it seriously, is enormously difficult.

1887   So I am very supportive of some of the initiatives we are

1888   seeing like bug bounties. So, for example, companies like

1889   BugCrowd are running many bug bounties where you as 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.

91

1890   organization can say if someone finds something wrong with my

1891   systems, I would like to know about it and I will likely pay a

1892   reward for that. And it is done legally, ethically, and it

1893   encourages the right behaviors.

1894   And I guess, finally, we'd also like to see more in the way

1895   of penalties because at the moment there's not enough

1896   accountability when things do go wrong, and I think we are all

1897   very curious to see how things like GDPR, which Mr. Grant mentioned

1898   earlier, how that plays out when it comes into effect in Europe

1899   in May where potentially an organization can be fined up to 4

1900   percent of their annual gross revenue.

1901   Now, that starts to sting and we really hope that that

1902   actually drives more positive behaviors in the industry.

1903   Mr. Griffith. All right. I appreciate that.

1904   Mr. Tonko? Ms. Castor?

1905   Appreciate you all being here. This has been very

1906   informative. I suspect it'll be one of the more popular reruns

1907   on CSPAN, for those folks who are really into this, and I have

1908   learned so much.

1909   Thank you all for your time today and I appreciate it.

1910   And with that, got to go to my script so I don't leave anything

1911   out. I would remind members that they have 10 business days 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.

1912   submit questions for the record and I ask that the witnesses all

1913   agree to respond promptly to those questions.

1914   Do I need to say anything else? All right. Got all that

1915   business -- housekeeping taken care of.

1916   With that, the subcommittee is adjourned. Thank you.

1917   [Whereupon, at 11:47 a.m., the committee was adjourned.]