

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

1 {York Stenographic Services, Inc.}

2 HIF125.170

3 HEARING ON ``H.R. 2221, THE DATA ACCOUNTABILITY AND

4 PROTECTION ACT, AND H.R. 1319, THE INFORMED P2P USER ACT''

5 TUESDAY, MAY 5, 2009

6 House of Representatives,

7 Subcommittee on Commerce, Trade, and Consumer Protection

8 Committee on Energy and Commerce

9 Washington, D.C.

10 The subcommittee met, pursuant to call, at 2:00 p.m., in
11 Room 2123 of the Rayburn House Office Building, Hon. Bobby L.
12 Rush (chairman) presiding.

13 Members present: Representatives Rush, Stupak, Barrow,
14 Radanovich, Stearns, Bono Mack, Terry, Murphy of
15 Pennsylvania, Gingrey and Scalise.

16 Staff present: Christian Fjeld, Counsel; Marc Gromar,
17 Counsel; Valerie Baron, Legislative Clerk; Brian McCullough,
18 Minority Senior Professional Staff; Will Carty, Minority
19 Professional Staff; and Sam Costello, Minority legislative

20 Analyst.

|
21 Mr. {Rush.} The subcommittee will now come to order.

22 Today the subcommittee is holding a legislative hearing
23 on two bills: H.R. 2221, the Data Accountability and Trust
24 Act, and H.R. 1319, the Informed P2P User Act. The chair
25 will recognize himself for 5 minutes for the purposes of an
26 opening statement.

27 Today the subcommittee is holding a legislative hearing
28 on the two above-mentioned bills. They were both introduced
29 by two distinguished members of the subcommittee, my
30 colleagues Ms. Bono Mack and Mr. Barrow, and H.R. 2221, which
31 is the Data Accountability and Trust Act, also known as DATA,
32 was introduced by myself and Mr. Stearns. Ms. Bono Mack and
33 Mr. Barrow introduced H.R. 1319. Both of these bills
34 represent strong bipartisan efforts to address high-profile
35 problems affecting American consumers.

36 H.R. 1319, the Informed P2P User Act, addresses the
37 increasingly frequent problem of consumers inadvertently
38 exposing their private sensitive information by way of peer-
39 to-peer file-sharing programs. Too often when consumers
40 download these programs onto their computers with the intent
41 of sharing and downloading certain files on the network, they
42 are unaware that they are also sharing other files they
43 otherwise might want to keep private. For instance, recent

44 media reports have focused on consumers unknowingly sharing
45 their tax returns and their Social Security numbers on P2P
46 networks. Such inadvertent file sharing can be the result of
47 deceptive or misleading disclosures by P2P software companies
48 or they might emanate from simple confusion on the part of
49 consumers. Whatever the case, the intent of H.R. 1319 is to
50 provide consumers with the power of informed consent before
51 they download P2P software onto their computers and share
52 folders and files with network participants.

53 The second bill that we will be discussing today is H.R.
54 2221, the Data Accountability and Trust Act. This is the
55 third Congress in which this bill has been introduced. Mr.
56 Stearns as chairman of this subcommittee in the 109th
57 Congress originally introduced the bill as H.R. 4127, and
58 with the help of then-Ranking Member Schakowsky, it
59 eventually passed the full Energy and Commerce Committee by a
60 unanimous vote. However, no further action was taken on the
61 bill as a result of jurisdictional disputes. In the
62 subsequent 110th Congress, I reintroduced the bill as H.R.
63 958, but we were unable to take any action. Once again in
64 this current Congress, I have reintroduced the bill with Mr.
65 Stearns, Mr. Barton, Ms. Schakowsky and Mr. Radanovich as
66 H.R. 2221 with the intent that it does eventually become law.

67 H.R. 2221 has two basic components. First, the bill

68 requires that persons processing electronic data that
69 contains personal information must take steps to ensure that
70 the data is secure. Second, the bill establishes a
71 notification procedure and process that a company must take
72 when a data breach occurs in order to allow affected
73 consumers to protect themselves. Companies do not have to
74 initiate such notices if they determine that ``there is no
75 reasonable risk of identify theft, fraud or other unlawful
76 acts.'' H.R. 2221 also imposes special requirements on data
77 brokers but accommodates other laws that govern how certain
78 data brokers are regulated. These bills may require some
79 revision, and while this may not be the first time we have
80 taken up data security, and H.R. 2221 already reflects
81 significant changes forged by compromise made in the 109th
82 Congress, the bill may be dated and in need of an update.
83 This subcommittee is looking forward to working in a
84 bipartisan fashion and seeking bipartisan cooperation based
85 on our historical bipartisanship, and I expect that
86 bipartisanship to be at work on both of these bills.

87 Lastly, I want to just announce for the record that I
88 have an intention to hold a joint hearing on consumer privacy
89 with Chairman Boucher and the Subcommittee on Communications,
90 Technology, and the Internet and to work on comprehensive
91 legislation. This is just a part of a larger process.

92 [The prepared statement of Mr. Rush follows:]

93 ***** COMMITTEE INSERT *****

|
94 Mr. {Rush.} With that, I yield back the balance of my
95 time and recognize now for the purposes of an opening
96 statement the ranking member on this subcommittee, Mr.
97 Radanovich, for 5 minutes.

98 Mr. {Radanovich.} Thank you, Mr. Chairman. Good
99 afternoon, everybody.

100 I would first like to thank the witnesses before us
101 today and the organizations that have offered comments and
102 suggestions assisting the important work of crafting a robust
103 and workable data security bill. Both that bill and the P2P
104 bill that we have, there are core concerns about the
105 unauthorized or inadvertent sharing of sensitive information.
106 I want to commend Mr. Stearns, Ms. Schakowsky, Mr. Barton,
107 Mr. Dingell, Mr. Whitfield and now Mr. Rush and Mr. Waxman,
108 all of whom were chairmen and/or ranking members who have
109 helped bring attention to these issues. I also want to
110 recognize Ms. Bono Mack's leadership on digital security over
111 the years and on her bill to prevent inadvertent file sharing
112 on peer-to-peer networks.

113 File sharing presents privacy and security issues but
114 also relates to online safety more generally, and being a
115 father, I am glad to see that a bill that improves children's
116 digital safety and will help protect from some of the

117 atrocities that are being committed using these networks on
118 line.

119 Huge data security breaches shocked us all starting back
120 in 2005 with the ChoicePoint breach and millions of people in
121 the United States had discovered that they are victims of
122 identify theft. Billions are lost by consumers and by
123 businesses as they spend money and time to repair their
124 finances. Particularly in difficult economic times when
125 credit is increasingly tough to secure, the potential
126 disruption and obstruction of commercial activity in every
127 sector of the U.S. economy cannot be ignored. Internet-based
128 and other electronic transactions are fundamental these days
129 and ensuring consumer confidence in these systems is
130 essential. The Congress, and this committee in particular,
131 are charged with the responsibility to ensure that the
132 entities possessing and dealing in sensitive consumer data
133 keep the doors locked and the alarm on.

134 The health of our modern network system of commerce
135 demands it. Very simply, H.R. 2221 would create a uniform
136 national data breach notification regime. I believe that
137 notification must be based on the actual risk of potential
138 harm from identify theft or other malfeasance and the
139 mandates that we put on covered entities must be the same
140 across the country. Allowing individual States to alter the

141 rules will only lead to consumer confusion and unnecessary
142 business expenses, costs that will inevitably be passed on to
143 the consumer. Let us get a good bill that robustly protects
144 consumers while not adding requirements that only add costs.

145 The world has changed since we last considered this
146 bill, and I am anxious to hear about those developments.
147 Some parts of the bill may now be obsolete, given the actions
148 of the private sector, actions by both those who hold
149 sensitive information and by companies who now offer products
150 directly to consumers to monitor their credit. We must take
151 all of this into account and get a workable bill that we can
152 all support.

153 While the data security bill is one with which the
154 committee has some experience, Ms. Bono Mack's bill, H.R.
155 1319, is a relatively new one. She was out in front on the
156 issue last Congress, introducing an earlier version of the
157 bill last September. Since then we have seen multiple news
158 stories about the problems the bill attempts to addressing,
159 inadvertent sharing of sensitive files across peer-to-peer
160 networks. I want to state at the outset that it is not the
161 committee's intent to simply demonize P2P software. There
162 are many legitimate and important uses of this innovative
163 program and I am glad that the P2P industry is here to talk
164 about the uses of their products. However, the systems

165 present some interesting problems as well. Last month the
166 P2P security company Tiversa, who is here to testify, found
167 the schematics of Marine One, President Obama's new
168 helicopter, on a P2P server in Iran. In other reporting it
169 was found that millions of sensitive personal records
170 including Social Security numbers, medical records, credit
171 reports and tax returns with names and addresses were easily
172 found on P2P networks.

173 The problem of inadvertent sharing is enhanced by the
174 actual architecture of the programs. It is often unclear to
175 a user what may be leaked, and it can be difficult to change
176 settings to prevent it. After Mr. Waxman examined this in
177 the former committee down the hall, it appears that 2 years
178 later many P2P providers have not taken adequate steps to
179 address this. We need to take a close look at the problem
180 and the bill. We do not want to sweep technologies into a
181 potential regime that we do not intend nor do we want to
182 exclude technologies that we can all agree should be covered.
183 How we define P2P software is critical.

184 Mr. Chairman, I look forward to the comments on these
185 bills and I would like to express my gratitude to the
186 majority for their intent to develop these bills. Thank you,
187 Mr. Chairman.

188 [The prepared statement of Mr. Radanovich follows:]

189 ***** COMMITTEE INSERT *****

|
190 Mr. {Rush.} The chair thanks the gentleman.

191 The chair now recognizes Mr. Barrow for 2 minutes. Mr.
192 Barrow is a sponsor of one of the bills and certainly I am
193 grateful to him for his legislative work. Mr. Barrow, you
194 are recognized for 2 minutes for the purposes of opening
195 statement.

196 Mr. {Barrow.} Thank you, Mr. Chairman.

197 We live in a world where digital technology has
198 connected people and their ideas, their information and
199 products, making possible all kinds of new kinds of
200 collaboration and innovation. There is no doubt that this
201 has made us all a lot more productive. It has also made it
202 possible for folks to invade our personal records and reveal
203 private information about us and our families that we choose
204 not to disclose.

205 The purpose of today's hearing is to discuss threats to
206 data security and ways we can work to fill in the gaps that
207 leave our personal records vulnerable. I had the opportunity
208 to work with Congresswoman Mary Bono Mack on H.R. 1319, the
209 Informed Peer to Peer User Act, and I hope that this hearing
210 will shed some light on the privacy and security risks that
211 are associated with peer-to-peer file-sharing programs. A
212 lot of folks who connect to these networks don't even realize

213 that their most personal and private files are visible to
214 everyone else on the network at any time. A lot of folks are
215 posting their tax returns, financial records and personal
216 messages on the Internet and don't even know it. I hope that
217 our work on this committee will come up with a strategy that
218 will let individuals know in a way that they can understand
219 and use that the information on the computers could be at
220 risk. We have truth in lending and we have truth in
221 labeling. I think it is time we had truth in networking
222 also.

223 I want to thank Congresswoman Mary Bono Mack for
224 allowing me to work with her on the Informed Peer to Peer
225 User Act and I want to thank Chairman Waxman and Ranking
226 Member Barton for bringing these important issues to the
227 forefront in our committee, and most importantly, I want to
228 thank every one of you on this panel today for being here to
229 lend your expertise on this important subject.

230 Thank you, and I yield back the balance of my time.

231 [The prepared statement of Mr. Barrow follows:]

232 ***** COMMITTEE INSERT *****

|
233 Mr. {Rush.} The chair thanks the gentleman. The chair
234 now recognizes the other author of one of these bills that we
235 are hearing today, Ms. Bono Mack--I am sorry--Mr. Stearns, I
236 am sorry, the former ranking member of the subcommittee, Mr.
237 Stearns of Florida, who is recognized for 2 minutes for the
238 purposes of an opening statement.

239 Mr. {Stearns.} Thank you, Mr. Chairman, and I--

240 Mr. {Rush.} I didn't mean to confuse you with Ms. Bono
241 Mack.

242 Mr. {Stearns.} She is much better looking.

243 Mr. Chairman, thank you very much, and I think in your
244 opening statement you pretty much outlined my feeling about
245 this. Obviously this is a bill that was introduced on
246 October 25, 2005. It was H.R. 4127, and as you pointed out,
247 we passed this bill by unanimous consent. Ms. Schakowsky and
248 I worked together on that bill and we had compromises. We
249 got the bill. So I am very pleased that you have taken the
250 initiative, the leadership the offer this bill again, and I
251 am very glad to be an original cosponsor with you. I am
252 hoping it has the same kind of success that we had, Ms.
253 Schakowsky and I, because it is a very, very important bill.

254 Recently some hackers broke into a Virginia State
255 website used by pharmacists to track prescription drug abuse.

256 They took all these names and it is 8 million patients and
257 they deleted them from the site and they are asking for money
258 to replace them, so in a way they are asking for ransom, and
259 if this Virginia website had an encrypted data security full-
260 blown protection of this information, it would have been
261 difficult, if not impossible, for these hackers to get in and
262 to take this information. It is 8,257,000 names. And that
263 is why this bill is so important so I am very pleased to
264 support it.

265 Also, the gentlelady from California's bill, the
266 Informed P2P User Act, which is again very important. With
267 the diverse connectivity we have in networks, and of course
268 with the increased broadband that we are starting to see,
269 people are going to go more to this peer-to-peer downloading
270 and this centralized resources in your computer and these
271 servers going back and forth between each other, you have got
272 to have some notification to the users what is occurring or a
273 lot of their applications and their information will be also
274 taken.

275 So it is very appropriate these two bills come together,
276 I think, and Mr. Chairman, I commend you and your staff for
277 bringing them both because in a way we are talking about data
278 security with both of them and protection of the consumer,
279 and I thank you, Mr. Chairman.

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

281 ***** COMMITTEE INSERT *****

|
282 Mr. {Rush.} The chair thanks the gentleman. Now the
283 chair recognizes Ms. Bono Mack of California for 2 minutes
284 for the purposes of an opening statement.

285 Ms. {Bono Mack.} I thank the chair and Ranking Member
286 Radanovich and the distinguished panel for being here today.
287 Thank you for holding a hearing on important privacy
288 legislation. Today my comments will focus entirely on H.R.
289 1219, the Informed P2P User Act, but before I dig into the
290 issue of P2P, I would like to thank Ranking Member Barton as
291 well as my colleague, Congressman Barrow, for their
292 willingness to work together on H.R. 1319. As you have seen,
293 this is a bipartisan bill and their support has been
294 essential. I thank them both.

295 The risks associated with peer-to-peer file-sharing
296 programs has been widely reported by the media and thoroughly
297 investigated by Congress. Many of our witnesses today have
298 testified before other Congressional committees on the
299 dangers associated with P2P file-sharing programs, and each
300 time the committee was given a status update of the dangers.
301 Additionally, industry claimed ignorance and stated they
302 would handle the problem through self-regulation. This
303 hands-off approach has not worked and any set of voluntary
304 best practices put forth by the P2P industry can no longer be

305 seen as credible. To paraphrase Groucho Marx, you want me to
306 believe you and your voluntary measures instead of my own two
307 eyes. How many more medical records and tax returns is it
308 going to take for us to act? How many state secrets will be
309 made available to those who want to harm us? How much more
310 damage are we going to allow P2P file-sharing programs to do
311 to our economy? I believe enough is enough and the time to
312 act is now.

313 Industry's opportunity to self-regulate has passed. P2P
314 file-sharing programs like Lime Wire and Kazaa before it have
315 proven they are either incapable of solving the problem of
316 inadvertent file sharing on their own or they have absolutely
317 no intention of solving the problem at all. Either way, this
318 behavior is unacceptable, as the committee charged with
319 consumer protection, we have a responsibility to our
320 constituents to act.

321 I am also aware that some of you have concerns about
322 some of the language of H.R. 1319. Please note that my
323 office is very willing to listen to your concerns and work
324 with you to craft a bill that is not overly broad but still
325 carries out the current intent of H.R. 1319. I believe that
326 if we work together we should be able to produce a bill that
327 protects our constituents and preserves the legitimate use of
328 P2P applications.

329 I look forward to today's discussion, and I thank the
330 chairman very much for holding this hearing. I yield back.

331 [The prepared statement of Ms. Bono Mack follows:]

332 ***** COMMITTEE INSERT *****

|
333 Mr. {Rush.} The chair thanks the gentlelady. Now the
334 chair recognizes the gentleman from Pennsylvania, Dr. Murphy,
335 for the purposes of opening statement. The gentleman is
336 recognized for 2 minutes.

337 Mr. {Murphy of Pennsylvania.} Thank you, Mr. Chairman,
338 and by the way, I would also like to welcome a Pittsburgher,
339 Mr. Boback of Tiversa, he and I have spoken a number of times
340 in the past, as well as this incredibly distinguished panel.
341 The expertise you all have, I am excited about you being
342 here.

343 The sad thing about this is, this is a discussion that
344 has not begun today. I think some of you have testified in
345 past years and I know that Mr. Boback and I have spoken years
346 ago. When we look at what has been released about the
347 documents from Marine One, a couple terabytes of information
348 on the Joint Strike fighter jet, a whole host of so much
349 information, it makes me wonder why anybody trusts to have
350 any files on the computers at all. It reminds me of the way
351 that Rome acted during the time the Barbarians were beginning
352 to invade various parts of Germany, and I am sure some Roman
353 emperor, some Roman generals were saying nothing to worry
354 about, we have this system under control, even when they were
355 sacking Rome, and I believe that is where we are now. It is

356 not safe. The portals created by these peer-to-peer networks
357 are huge and the fact that our Department of Defense keeps
358 anything on any computer that is accessible from the outside
359 still astounds me. I applaud this bill, and I think this is
360 important because it does move a long way towards protecting
361 consumers and families who inadvertently have their files
362 stolen and accessed whether it is their tax records, medical
363 records or anything else. But the best thing we need to
364 remember for so many folks whether they are John and Jane Doe
365 in their home somewhere or it is our defense department or is
366 any corporation that no matter what we do here, they are
367 still responsible for keeping the information inaccessible to
368 the Internet because those folks from other countries who
369 continue to send out press releases denying they are doing it
370 and yet all paths seem to lead back to those countries, we
371 have to understand that the wealth of information we have on
372 our computer networks and what we have done to protect those
373 is all for naught if we continue to put those on computers.

374 With that, Mr. Chairman, I yield back.

375 [The prepared statement of Mr. Murphy of Pennsylvania
376 follows:]

377 ***** COMMITTEE INSERT *****

|
378 Mr. {Rush.} The chair thanks the gentleman. Now the
379 gentleman from Nebraska, Mr. Terry, is recognized for 2
380 minutes for the purposes of an opening statement.

381 Mr. {Terry.} Thank you, Mr. Chairman. I want to thank
382 you for holding today's hearing, but more specifically, we
383 have been down this road a couple times before and I think it
384 is imperative that we move these bills.

385 I am going to pile on a little bit Mr. Murphy's comments
386 that I view this as nibbling around the edges of
387 cybersecurity. We are pointing to specific problems and
388 trying to come up with specific solutions. All the while we
389 are losing sight of the forest. I am not saying these
390 shouldn't be done but I just think we need to think about in
391 a grander scheme of cybersecurity and how it all ties in with
392 our national security now, our financial security, and
393 hopefully we can start elevating the level of discussion here
394 but I want to congratulate the authors of both of the bills
395 here. I think you have done a decent job here of finding the
396 right solution for these specific problems and I support
397 them. Yield back.

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

399 ***** COMMITTEE INSERT *****

|
400 Mr. {Rush.} The chair thanks the gentleman and now the
401 chair recognizes the gentleman from Georgia, Dr. Gingrey, for
402 2 minutes for the purposes of an opening statement.

403 Mr. {Gingrey.} Mr. Chairman, thank you for calling this
404 hearing today that focuses on two bipartisan pieces of
405 legislation, H.R. 2221, the Data Accountability and Trust
406 Act, and H.R. 1319, the Informed Peer to Peer User Act. I
407 also want to commend both you and Ranking Member Radanovich
408 for your collective leadership and for the spirit of comity
409 in which this subcommittee is operating, Mr. Chairman.

410 At a time when our society is becoming ever more reliant
411 on technology, whether for e-commerce or HIT, health
412 information technology, we need to ensure the security of an
413 individual's identity and personal information.
414 Unfortunately, we have seen significant breaches of
415 information that have led to identify theft, fraud and
416 allegations that were first reported in the Wall Street
417 Journal that Chinese hackers--it is bad enough what Ranking
418 Member Stearns was saying about the pharmaceutical and
419 prescription drug information but Chinese hackers stole
420 several terabytes of data related to design and electronic
421 systems of the Joint Strike fighter. That is some serious
422 business.

423 H.R. 2221 is legislation that was first written in the
424 109th Congress by my colleague from Florida, Mr. Stearns. It
425 is now being spearheaded by you, Mr. Chairman, and I applaud
426 you on this effort. This legislation requires entities
427 holding data that contains personal information to implement
428 enhanced security measures to prevent future breaches. In
429 instances in which unauthorized access does occur, then the
430 consumers must be notified shortly thereafter that their
431 files were compromised.

432 Similarly, H.R. 1319 is legislation that was introduced
433 by Ms. Bono Mack of California, full committee Ranking Member
434 Barton and my colleague from Savannah, Georgia, Mr. Barrow,
435 and it is designed to protect consumers through additional
436 information about the practice of peer-to-peer file sharing
437 over the Internet. Simply referred to as P2P file sharing
438 around the IT industry, this practice certainly has a number
439 of benefits. However, too often personal information is
440 compromised over the peer-to-peer program for various
441 reasons, many of which of course are inadvertent. H.R. 1319
442 would add an additional layer of security that would prohibit
443 peer-to-peer programs from sharing files until the program
444 receives informed consent from the user on two separate
445 occasions.

446 Mr. Chairman, we need to maintain security on the

447 Internet in this growing technologically-based world, and I
448 do support both bipartisan bills. I look forward to hearing
449 from the witnesses, and I yield back.

450 [The prepared statement of Mr. Gingrey follows:]

451 ***** COMMITTEE INSERT *****

|
452 Mr. {Rush.} The chair thanks the gentleman and the
453 chair thanks all the members of the subcommittee for their
454 opening statements.

455 It is now my pleasure to introduce our outstanding
456 expert panel. These panelists have come from far and near to
457 be with us today, and we certainly welcome them and we
458 certainly want to tell each and every one of you beforehand
459 that we thank you so much for taking the time out from your
460 busy schedule to participate with us in this hearing.

461 I would like to first of all introduce you now. From my
462 far left is Ms. Eileen Harrington. Ms. Harrington is the
463 acting director of the Bureau of Consumer Protection for the
464 Federal Trade Commission. Next to Ms. Harrington is Mr.
465 David M. Sohn, who is the senior policy counsel for the
466 Center for Democracy and Technology. Next to Mr. Sohn is Mr.
467 Robert W. Holleyman, II. Mr. Holleyman is the president and
468 CEO of Business Software Alliance. Seated next to him is Mr.
469 Martin C. Lafferty. He is the chief executive officer of
470 Distributed Computing Industry Association. Next to Mr.
471 Lafferty is Mr. Stuart K. Pratt, president and CEO of the
472 Consumer Data Industry Association, and then next to him is
473 Mr. Marc Rotenberg, who is the executive director of the
474 Electronic Privacy Information Center. The gentleman next to

475 Mr. Rotenberg is Mr. Robert Boback. He is the CEO of
476 Tiversa, Incorporated. And lastly but not least, the
477 gentleman seated next to Mr. Boback is Mr. Thomas D. Sydnor.
478 He is the senior fellow and director of the Center for the
479 Study of Digital Property of the Progress and Freedom
480 Foundation.

481 Again, I want to thank each and every one of the
482 witnesses for appearing today. It is my pleasure to extend
483 to you 5 minutes for the purposes of opening statement, and
484 we will begin with Ms. Harrington.

|
485 ^STATEMENTS OF EILEEN HARRINGTON, ACTING DIRECTOR, BUREAU OF
486 CONSUMER PROTECTION, FEDERAL TRADE COMMISSION; DAVID M. SOHN,
487 SENIOR POLICY COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY;
488 ROBERT W. HOLLEYMAN, II, PRESIDENT AND CHIEF EXECUTIVE
489 OFFICER, BUSINESS SOFTWARE ALLIANCE; MARTIN C. LAFFERTY,
490 CHIEF EXECUTIVE OFFICER, DISTRIBUTED COMPUTING INDUSTRY
491 ASSOCIATION; STUART K. PRATT, PRESIDENT AND CHIEF EXECUTIVE
492 OFFICER, CONSUMER DATA INDUSTRY ASSOCIATION; MARC ROTENBERG,
493 EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER;
494 ROBERT BOBACK, CHIEF EXECUTIVE OFFICER, TIVERSA, INC.; AND
495 THOMAS D. SYDNOR, SENIOR FELLOW AND DIRECTOR, CENTER FOR THE
496 STUDY OF DIGITAL PROPERTY, PROGRESS AND FREEDOM FOUNDATION

|
497 ^STATEMENT OF EILEEN HARRINGTON

498 } Ms. {Harrington.} Thank you very much, Chairman Rush,
499 Ranking Member Radanovich and members of the subcommittee. I
500 am Eileen Harrington, the acting director of the FTC's Bureau
501 of Consumer Protection. I appreciate the opportunity to
502 appear to present the Commission's testimony on data security
503 and peer-to-peer file sharing. The Commission's views are
504 set forth in its written testimony. My oral presentation and
505 answers to your questions represent my views.

506 Let me start with data security. Companies must protect
507 consumers' sensitive data. If they don't, that data could
508 fall into the wrong hands, resulting in fraud and consumers
509 losing confidence in the marketplace. The Commission has
510 undertaken substantial efforts described fully in its written
511 testimony to promote data security. Let me highlight three
512 particular efforts for you: our law enforcement activities,
513 our pending rulemaking on health information security and our
514 study of emerging technologies.

515 Today the Commission announced its 26th law enforcement
516 action against a business that we allege failed to have
517 reasonable procedures to protect consumers' personal
518 information. Case number 26 is against mortgage broker James
519 Nutter and Company for allegedly failing to implement basic
520 computer security measures. In settling these charges, the
521 company has agreed to maintain reasonable security measures
522 in the future and to periodic outside audits of its security
523 practices. The Commission's data security cases are well
524 publicized and send a strong message to the business
525 community: you must have reasonable data security measures
526 in place.

527 Second, a few weeks ago the Commission issued a proposed
528 rule to require that consumers be notified when the security
529 of their health information is breached. The proposed rule

530 arises from a mandate in the Recovery Act to address new
531 types of web-based entities that collect or handle consumers'
532 sensitive health information. Covered entities include those
533 that offer personal health records which consumers can use as
534 an electronic individually controlled repository for their
535 medical information. Personal health records have the
536 potential to provide numerous benefits for consumers but only
537 if they have confidence that the security of the health
538 information they put it in will be maintained.

539 Third, the Commission continues to examine new
540 technologies to identify emerging privacy and data security
541 issues. In February, for example, the Commission staff
542 released a report recommending principles for industry self-
543 regulation of privacy and data security in connection with
544 behavioral advertising. We are also considering a petition
545 submitted by EPIC raising data security concerns about cloud
546 computing services provided by Google.

547 Finally, a few words about the proposed data security
548 bill, H.R. 2221. The Commission strongly supports the goals
549 of the legislation, which are to require companies to
550 implement reasonable security procedures and provide security
551 breach notification to consumers. We also strongly support
552 the provisions that would give the Commission the authority
553 to obtain civil penalties for violations. We have provided

554 technical comments to committee staff, particularly with
555 regard to the scope of the proposed legislation and the data
556 broker provisions and very much appreciate the opportunity to
557 provide input.

558 Turning to P2P file sharing, let us be clear about one
559 thing. The FTC's interest is the safety and privacy of
560 consumers' personal documents and information, not copyright
561 piracy. Although P2P technologies may offer benefits to
562 computing, they have also been associated with significant
563 data security risks. The press has reported disturbing
564 instances of sensitive documents being shared via P2P
565 networks. Sensitive documents likely have been shared under
566 three scenarios. First, some consumers may have shared
567 documents because they failed to read or understand
568 information about how to keep files from being shared or did
569 not understand the consequences of altering default settings.
570 Second, some consumers may have unknowingly downloaded
571 malware that caused their files to be made available on P2P
572 networks. Third, some businesses and other organizations
573 that hold sensitive personal information such as tax or
574 medical records have not implemented procedures to block
575 installation of P2P file-sharing software on their company or
576 organization-owned computers and networks. Some of the most
577 highly publicized instances of personal information being

578 shared over P2P networks occurred because businesses failed
579 to prevent the installation of P2P software on their systems
580 or because their employees placed sensitive corporate
581 documents onto home computers that had downloaded P2P
582 software.

583 The FTC has worked with the P2P industry as it has set
584 standards for disclosure and default settings that protect
585 consumers' files and information. We have received reports
586 about the performance of seven P2P companies and are
587 currently reviewing them to see whether these companies
588 comply with the industry standards. We will make the results
589 of our review public this summer. We also educate consumers
590 about the risks associated with these programs. In addition
591 to a 2008 consumer alert, the FTC's Internet website,
592 onguardonline.gov, highlights information about the risks of
593 P2P file-sharing software.

594 Finally, we support legislation that requires
595 distributors of P2P file-sharing programs to provide timely,
596 clear and conspicuous notice and obtain consent from
597 consumers regarding the essential aspects of those programs.
598 H.R. 1319 may provide very useful protections for consumers.
599 The agency has worked with committee staff on previous
600 versions of the bill and we look forward to working with
601 committee staff again regarding this proposed legislation,

602 and we thank you very much for giving the FTC the opportunity
603 to present its views today.

604 [The prepared statement of Ms. Harrington follows:]

605 ***** INSERT 1 *****

|
606 Mr. {Rush.} The chair now recognizes Mr. Sohn for 5
607 minutes.

|
608 ^STATEMENT OF DAVID M. SOHN

609 } Mr. {Sohn.} Chairman Rush, Ranking Member Radanovich,
610 members of the subcommittee, thank you for the opportunity to
611 participate in today's hearing. The Center for Democracy and
612 Technology is very pleased to see this subcommittee focusing
613 on data privacy and security issues. Based on my
614 conversations with subcommittee staff, I am going to focus my
615 comments this afternoon on the Data Accountability and Trust
616 Act with just a few words at the end about the Informed P2P
617 User Act.

618 But before I do that, I would like to make a general
619 point. Both of the bills that are the focus of today's
620 hearing reflect the fact that technology has greatly expanded
621 the ability to collect, store, use and share personal data.
622 The modern information economy that this makes possible has
623 many benefits but it also has greatly changed the privacy
624 landscape and it has expanded the risk of inappropriate
625 disclosure of personal data. Unfortunately, the law has
626 simply not kept pace with these changes. In particular, the
627 United States has no general privacy law establishing any
628 kind of fair baseline of principles or expectations to govern
629 consumer privacy, and in the absence of that kind of overall

630 legal framework, when new privacy issues arise, Congress is
631 essentially left to legislate on a one-off basis without any
632 clear guiding principles and without necessarily much
633 consistency. The result, what we have today, is a confusing
634 patchwork of laws in this area. So based on that, CDT would
635 certainly urge the subcommittee to put a high priority on the
636 enactment of baseline federal privacy legislation and we are
637 very happy to hear Chairman Rush saying today that he plans a
638 joint hearing and does plan to work on comprehensive privacy
639 legislation.

640 Now I would like to turn to the Data Accountability and
641 Trust Act. CDT supports the idea of a nationwide data breach
642 notification standard so long as that standard is as least as
643 effective as the laws already in place at the State level.
644 The key point to understand here is that data breach
645 notification is already the law of the land because it is
646 required by all but a few of the States. So from a consumer
647 perspective, replacing State notification laws with a weak
648 federal standard could actually be a step backwards, and even
649 replacing them with a good federal standard still doesn't
650 offer a lot of tangible progress. The principal consumer
651 gains from H.R. 2221 therefore come from section 2 of the
652 bill, namely the provision for requiring data security
653 procedures and especially the provisions requiring

654 information brokers to let consumers review what is in their
655 data broker files. Based largely on these provisions, the
656 CDT does support the framework set forth in the bill.

657 My written testimony offers some suggestions for
658 improvements to the bill. For example, the breach
659 notification provisions could be improved by requiring a
660 company that suffers a breach but determines that there isn't
661 enough risk to notify consumers to nonetheless provide a
662 brief explanation to a regulator basically just to keep
663 everybody honest. For the provisions on security standards
664 and consumer access to information broker files, CDT
665 recommends taking a close look at the scope of those
666 requirements. In particular, the bill uses a definition of
667 personal data that is really quite limited, which may make
668 sense for breach notification provisions but might make less
669 sense for the provisions in section 2.

670 Preemption deserves a mention as well. It is important
671 to note that preempting State laws in this area is a very
672 significant step. The only reason we are here talking about
673 breach notification today is that notification laws were
674 pioneered by the States and especially California. States
675 were able to do that because the Gramm-Leach-Bliley Act
676 preempted inconsistent State laws but otherwise left States
677 free to experiment. Fortunately, the authors of H.R. 2221

678 have been careful with preemption. CDT does believe that
679 preemption makes sense for the specific issue of breach
680 notification and the bill does provide for that. I would
681 just say that as the bill moves forward, Congress needs to
682 keep in mind that the price of preemption must be strong
683 federal action and that overbroad preemption has to be
684 avoided. Overall, CDT does appreciate the careful work of
685 Chairman Rush and the other sponsors of this bill and we
686 stand ready to cooperate with them on possible improvements
687 as the bill moves forward.

688 Finally, just a couple words on the Informed P2P User
689 Act. CDT absolutely supports the principle that file-sharing
690 software should clearly communicate to users how their files
691 may be made available to third parties. Inadvertent sharing
692 of personal files is a very serious privacy matter. As set
693 forth in my written testimony, however, legislating this area
694 does pose some difficulties. CDT has reservations about the
695 potential unintended breadth of the bill and also has some
696 reservations about Congress starting down the path of
697 imposing specific design mandates for software developers.
698 That said, we share the broad goal and my written testimony
699 offers some ideas for modifications to consider if the
700 subcommittee chooses to proceed with the bill.

701 Thanks again for the opportunity to testify.

702 [The prepared statement of Mr. Sohn follows:]

703 ***** INSERT 2 *****

|
704 Mr. {Rush.} The chair thanks the gentleman. The chair
705 recognizes now for 5 minutes of opening statement Mr.
706 Holleyman.

|
707 ^STATEMENT OF ROBERT W. HOLLEYMAN, II

708 } Mr. {Holleyman.} Mr. Chairman, Ranking Member
709 Radanovich, other members of this subcommittee, I want to
710 thank you for the opportunity to testify today. The Business
711 Software Alliance represents the leading developers of
712 software and hardware. Of the software that is sold around
713 the world, roughly 90 percent of that is from companies who
714 are U.S.-based companies and our members believe strongly
715 that the type of inquiry that this committee is engaged in
716 today is important not only to ensure that our customers are
717 using software properly but also to ensure that the promise
718 of electronic commerce and equally important the promise for
719 the type of sensitive data that the government will hold and
720 does hold that we could have greater confidence because that
721 will add enormous efficiencies to our system.

722 As we look at the issue of breaches, the data is
723 astounding in terms of the problems that we have seen. I
724 won't repeat all of the information that has been so widely
725 covered in the press and by the subcommittee except that I
726 will note that the trend is that data breaches are growing.
727 In 2008, it is estimated that there was a 47 percent increase
728 in data breaches over the prior year, and the average cost of

729 each breach is growing, and for the ninth year in a row,
730 identify theft has topped the list of FTC consumer
731 complaints, about 26 percent of all their complaints, and
732 according to the Privacy Rights Clearinghouse, a staggering
733 270 million records containing sensitive personal information
734 have been affected since 2005. And certainly we have heard
735 on this panel today, we have heard in your opening statements
736 about Heartland Payment Systems, the single largest fraud-
737 related data loss ever in the United States. Estimates of
738 over \$100 million individual credit and debit card accounts
739 were compromised and the consequences of that have been
740 enormous.

741 And finally, to the point that I made about the
742 importance of government data, nearly 20 percent of all data
743 breaches involve government, federal, State and local
744 governments, and as we move to the promise of governments
745 holding even more sensitive data regarding our health records
746 as people live longer, as our population grows, as we build
747 the kind of openness and confidence in government, we have to
748 ensure that that important nexus is also protected.

749 With that, Mr. Chairman, I would like to comment on your
750 pending bill. We believe that this bill, Mr. Rush, makes
751 significant contributions to restoring and building a goal of
752 consumer citizen trust. We support its effort to establish a

753 uniform national standard and provide the preemption of State
754 laws. We also believe that it is important to recognize that
755 it would prevent excessive notification. We do need
756 notification but not all breaches are equal, and part of what
757 we need both in business but part of what consumers need is
758 to ensure that when the notification occurs, it is the result
759 of something that is meaningful. Third, we support exempting
760 from notification data that has been rendered unusable,
761 unreadable and indecipherable. We would recommend that the
762 limitation in the bill that refers to encryption be broader
763 so that we are looking at what the test is, and really this
764 creates market-based incentives that supplement the
765 regulatory authority that is given. It is that combination
766 that will ensure that more holders of data ensure that even
767 if there is a breach, that the party that has carried out the
768 breach or the unlawful entity can't do anything with that
769 data, and that is an important safeguard. Fourth, we believe
770 that your bill takes an appropriate risk-based approach to
771 securing data and we support the grant of authority and would
772 recommend that it be limited to the FTC and State attorneys
773 general rather than extending a private right of actions.

774 A couple of comments about H.R. 1319. We welcome this
775 effort by Ms. Bono Mack and other members of the subcommittee
776 to address this issue. Consumer privacy can be and is being

777 compromised because of certain peer-to-peer file-sharing
778 applications. We also appreciate this subcommittee's
779 willingness, the committee's willingness to look at the
780 current breadth of this bill to identify where it could be
781 appropriately limited. We do believe that there are two
782 goals in this. One is to protect consumer security and
783 promote trust and the second is to ensure that technological
784 innovation continues to proceed. It is this balance that
785 must be struck and it must be struck carefully. We are all
786 concerned that the bill, if it is in its current form, could
787 pull in some of the very legitimate applications and uses of
788 peer-to-peer technology that are important for every
789 consumer, important for legitimate companies. As it seeks to
790 look at some of the bad actors or some of the peer-to-peer
791 software that we widely know as an anti-piracy organization
792 that have led to the widespread theft of software, music,
793 movies and other content, we also know that the bill in its
794 current form could sweep in any Internet-aware features of
795 software such as automatic updates for anti-virus software
796 such as the crash analysis feature of operating systems or
797 the web browsers on our computers. We know that that is not
798 the intent of this bill but as written it could reach that
799 breadth, and so we would urge the committee to recognize that
800 while some effort should be made, it is important to enhance

801 security. We also want to ensure that the technological
802 progress and growth proceeds and that will benefit all users
803 of legitimate software.

804 So on behalf of BSA, thank you for this opportunity and
805 look forward to your questions.

806 [The prepared statement of Mr. Holleyman follows:]

807 ***** INSERT 3 *****

|
808 Mr. {Rush.} The chair thanks the gentleman. The Mr.
809 Chairman, Mr. Lafferty, for 5 minutes.

|
810 ^STATEMENT OF MARTIN C. LAFFERTY

811 } Mr. {Lafferty.} Chairman Rush, Ranking Member
812 Radanovich, subcommittee members, thank you for holding this
813 important hearing. I am Marty Lafferty, CEO of the
814 Distributed Computing Industry Association.

815 Both of the bills under consideration have far-reaching
816 consequences. Our expertise relates primarily to H.R. 1319.
817 DCIA is a trade group focused on P2P and related
818 technologies. Our mission is to foster commercial
819 development of these technologies so that their benefits can
820 be realized by all participants in the distribution chain
821 including content rights holders and Internet service
822 providers. We currently have 125 member companies including
823 P2P, cloud computing, file sharing and social network
824 software distributors, broadband operators, content providers
825 and service and support companies. P2P has evolved greatly
826 in the 8 years since Napster first brought the term P2P file
827 sharing to prominence. Fully licensed ad-supported P2P,
828 subscription P2P, paid download P2P, commercial enterprise
829 P2P, P2P TV, hybrid P2P and live P2P streaming now deserve to
830 be separated from the narrow subset of functionality
831 associated with file sharing. DCIA member companies

832 increasingly use P2P for the delivery of authorized
833 entertainment and corporate communications content where
834 rights holders rather than end users introduce files or live
835 streams for online delivery. We strongly urge the committee
836 to apply the term ``file sharing'' without the P2P prefix as
837 a more accurate descriptor for the focus of H.R. 1319.

838 The Committee on Oversight and Government Reform held a
839 hearing on this topic in July 2007 at which one of our member
840 companies testified. Within weeks of that hearing, the DCIA
841 established the Inadvertent Sharing Protection Working Group.
842 Over several months we recruited participants among leading
843 P2P and other tech sector companies and engaged with FTC
844 staff to address issues associated with unintended publishing
845 of confidential data by file sharers. This effort began by
846 providing demonstrations for FTC staff of how current file
847 share programs work in terms of users uploading material for
848 distribution. It continued through a process involving
849 private sector and regulatory participants to develop a
850 program of voluntary best practices for file-sharing software
851 developers to protect users against inadvertently sharing
852 personal or sensitive data. This program was announced in
853 July of 2008. Its summary, included in our written
854 testimony, begins by defining terms relevant to 1319 such as
855 recursive sharing, sensitive file types and user-originated

856 files. It then outlines seven steps that are required to be
857 in compliance: default settings, file-sharing controls,
858 shared folder configurations, user error protections,
859 sensitive file type restrictions, file sharing status
860 communications and developer principles. The principles
861 address feature disablement, uninstallation, new version
862 upgrades and file-sharing settings. In August 2008, the DCIA
863 announced that compliance monitoring would begin in December
864 to allow developers time to integrate required elements of
865 the ISPG program into their planned upgrades and new
866 releases. Compliance monitoring resulted in reports from top
867 brands that use P2P for downloading, live streaming, open
868 environment sharing and corporate Internet deployments and
869 for both user-generated and professionally produced content.
870 Specifically, seven leading P2P representative program
871 distributors submitted detailed reports to FTC staff in
872 February 2009. In March the DCIA prepared and submitted a
873 summary. We also noted that software implementations of the
874 popular BitTorrent protocol typically require users to
875 conduct a deliberate conversion process from whatever native
876 file format their content is in to a torrent file before it
877 can be published, thus minimizing this risk of user error.
878 The entire report plus data tables of individual company
879 submissions are in our written testimony but here are

880 highlights.

881 All respondents now have clearly disclosed install
882 default settings that only permit sharing files downloaded
883 from the network. They do not share user-generated files by
884 default. A hundred percent also provide complete
885 uninstallation of their file-sharing software that is simple
886 to do and explained in plain language, for example, by using
887 the standard add/remove program in Windows. And six out of
888 seven, which is all where this is applicable, now offer a
889 simple way to stop sharing any folder, subfolder or file by
890 using easily accessed controls.

891 In April 2009, subcommittee staff invited the DCIA to
892 participate in redrafting H.R. 1319. We formed a DCIA member
893 subgroup to conduct this work. The process is underway and
894 we are glad to coordinate that work with staff. Among our
895 greatest concerns is that the bill as drafted would have
896 unintended consequences. The present draft goes way beyond
897 the specific concerns discussed here and would apply to
898 additional functionality and technologies that have nothing
899 to do with recursive sharing of sensitive file types.
900 Applying these requirements to numerous products, services
901 and companies would be burdensome and counterproductive. To
902 the extent that legitimate consumer concerns persist in the
903 area that the bill intends to address, we strongly believe

904 they can best be handled by ongoing self-regulation under the
905 oversight of the appropriate federal authority as we
906 initiated with the ISPG.

907 The bill as constructed would unnecessarily burden U.S.-
908 based technology firms with innovation freeze and constraints
909 while being unenforceable against overseas competitors'
910 software available to U.S. consumers. The great concern also
911 is how it might stifle yet undeveloped new and potentially
912 very useful and valuable software applications. On the other
913 hand, the DCIA has committed to self-regulation through the
914 ISPG to address the subject matter of this bill and is making
915 substantial progress. So rather than a problematic new legal
916 measure, we believe that formalized requirements for
917 compliance with that process will be more effective in
918 achieving the purpose of the bill.

919 We look forward to working with the subcommittee on
920 these issues in a productive manner and will benefit all your
921 constituents. Thank you for your continued interest in our
922 industry.

923 [The prepared statement of Mr. Lafferty follows:]

924 ***** INSERT 4 *****

|
925 Mr. {Rush.} The chair thanks the gentleman. The chair
926 now recognizes Mr. Pratt for 5 minutes for the purposes of an
927 opening statement.

|
928 ^STATEMENT OF STUART K. PRATT

929 } Mr. {Pratt.} Chairman Rush, Ranking Member Radanovich
930 and members of the subcommittee, thank you for this
931 opportunity to appear before you today. My name is Stuart
932 Pratt, president and CEO of the Consumer Data Industry
933 Association. Our 250 member companies provide our Nation's
934 businesses with data tools necessary to manage risk and a
935 wide range of consumer transactions, and these products
936 include credit, mortgage reports, identify verification
937 tools, law enforcement investigative products, fraud check
938 transaction identification systems, decision sciences
939 technologies, location services and collections. My comments
940 today will focus exclusively on H.R. 2221, and we applaud its
941 introduction.

942 CDIA's members agree that sensitive personal information
943 should be protected. We also agree that consumers should
944 receive breach notices when there is a significant risk of
945 them becoming victims of identify theft. Our members agree
946 with the Federal Trade Commission recommendations which
947 embrace these two concepts. I would only add that if a
948 federal law is to be enacted, it should be a true national
949 standard.

950 We believe that data security and breach notification
951 provisions in H.R. 2221 would be most effective if they were
952 better aligned with requirements found in other current laws.
953 Alignment is key to ensuring that all who are affected by the
954 Act are successful in complying with new duties under DATA
955 and also with their current duties found under other laws
956 such as the Fair Credit Reporting Act and the Gramm-Leach-
957 Bliley Act. Let me discuss some of the ways that 2221
958 interplays with existing duties found in current laws.

959 Section 56 defines the term ``information broker.''
960 Absent aligning this definition with other current laws, our
961 members' products will be affected. This bill would require
962 information brokers to have reasonable procedures to verify
963 the accuracy of personal information, provide consumers with
964 access to these data and ensure a system by which consumers
965 can dispute information. All of our members operate consumer
966 reporting agencies as this term is defined in the Fair Credit
967 Reporting Act. They produce data products defined as
968 consumer reports. Consumer reports are used to make
969 determinations of a consumer's eligibility for a service or a
970 product and the FCRA establishes duties for accuracy, access
971 and correction as it relates to these products. Our members
972 agree that where data is used to make a decision regarding
973 consumers' eligibility for a product or service, consumers

974 should have these rights.

975 Since there are similar duties under the FCRA and DATA,
976 we propose the definition of information broker should be
977 amended to exclude the term ``consumer reporting agency'',
978 and while we appreciate the inclusion of section C3C which
979 attempts to address our concern, we believe that since the
980 FCRA's duties are well understood and the FTC has direct
981 enforcement powers, that we should have a complete exemption.

982 Regarding disclosure, section C3 allows an information
983 broker under certain circumstances to not disclose personal
984 information to a consumer. This section does not exempt an
985 information broker's fraud prevention tool from the duty to
986 verify accuracy. Fraud prevention tools are designed to
987 identify the possibility of fraud and to apply an accuracy
988 standard of fraud prevention tools is unworkable since these
989 tools are designed to warn a lender or utility or other
990 business about the possibility of fraud. Fraud prevention
991 tools consider how data has been used in previous identified
992 cases of fraud and employ many other relational strategies.
993 We would urge the expansion of C3B to include fraud
994 prevention tools so that they are completely exempted from
995 the accuracy standard requirement, not because the tools are
996 designed poorly but because these tools cannot line up with
997 an accuracy standard in the first place.

998 Your bill also as indicated establishes both a
999 requirement for data security and a requirement for security
1000 breach and we have absolutely no qualms about either of those
1001 requirements. Our member in fact comply with those types of
1002 requirements today and our only request is that where our
1003 member companies are already operating as a consumer
1004 reporting agency under the Fair Credit Reporting Act or where
1005 they are operating as a financial institution under the
1006 Gramm-Leach-Bliley Act, that they would be exempted from
1007 these data security and these security breach notification
1008 duties because they already have those duties under the Fair
1009 Credit Reporting Act and also under the Gramm-Leach-Bliley
1010 Act and in particular the safeguards rules which include
1011 breach notification.

1012 So this process of alignment will make this bill more
1013 effective. If we can make this truly a national standard,
1014 you certainly will have filled some gaps along the way. I
1015 think that Mr. Sohn said it very well. In the meantime, we
1016 live with a range of State laws. We have worked
1017 constructively with many, many States in establishing those
1018 statutes and in establishing definitions of the crime of
1019 identify theft and we will continue to do that and we look
1020 forward concurrently to working with you in the committee.
1021 Thank you.

1022 [The prepared statement of Mr. Pratt follows:]

1023 ***** INSERT 5 *****

|
1024 Mr. {Rush.} The chair thanks the gentleman, and now the
1025 chair recognizes Mr. Rotenberg for 5 minutes.

|
1026 ^STATEMENT OF MARC ROTENBERG

1027 } Mr. {Rotenberg.} Mr. Chairman, Mr. Radanovich, members
1028 of the committee, thank you very much for the opportunity to
1029 be here today. EPIC is a nonprofit research organization
1030 here in Washington.

1031 We have a particular interest in this issue of security
1032 breach notification. EPIC was the organization that had
1033 urged the Federal Trade Commission to investigate the data
1034 practices of a company called ChoicePoint because we believed
1035 that that company was making the personal information of
1036 American consumers vulnerable to misuse. The FTC did not
1037 heed our warning and instead we all read in the newspapers
1038 when an investigation broke in Los Angeles that revealed that
1039 the records of 145,000 American consumers had been sold to a
1040 criminal ring engaged in the act of identify theft. I
1041 promise you, after that news story appeared, the FTC and many
1042 State attorneys general became very interested in this
1043 problem.

1044 Now, we learned of the problem with ChoicePoint in part
1045 because of a good law that had been passed in the State of
1046 California which required companies that suffered from a
1047 security breach to notify people who are impacted, and as a

1048 result of the ChoicePoint notification, many other States
1049 began to understand the need for security breach
1050 notification. Now, this has been an evolving process. I
1051 think there are now 44 States in the United States that have
1052 security breach notification, and while we certainly support
1053 an effort to establish a high standard across the country, I
1054 do want to warn you that one of the consequences of this bill
1055 would be to effectively tie the hands of the State from
1056 further updating their laws or enforcing stronger laws, and I
1057 think this would be a mistake. I read recently, for example,
1058 that the California State Senate has just approved new
1059 changes to its notification law that would provide
1060 individuals with better information about the type of
1061 personal information that was improperly disclosed and how it
1062 might be misused. This need to be able to continue to update
1063 security breach notification I think should be a
1064 consideration as the committee looks at legislation to
1065 establish a national standard.

1066 One of the other points I would like to make about the
1067 legislation concerns the relationship in the realm of
1068 notification between the individuals who are impacted and the
1069 role of the Federal Trade Commission, which is also notified
1070 under the bill. There is understandable concern that if
1071 individuals receive too many breach notices, they will serve

1072 no purpose, and so there is a need to set a standard so that
1073 people are not receiving lots and lots of these notices which
1074 they will come to ignore. But with respect to the role of
1075 the Federal Trade Commission, I think the bill could be
1076 strengthened by requiring companies in all circumstances to
1077 notify the Commission where substantive breaches have
1078 occurred, and moreover to put on the Commission an obligation
1079 to be more transparent about the information that it receives
1080 regarding the problems of breach notification in the United
1081 States. There is also a risk with the legislation as it is
1082 currently drafted that the FTC will obtain information about
1083 security breaches, may choose not to act on the information
1084 it receives and that information will effectively remain
1085 secret both to the public and to this committee and the
1086 problem will continue to grow, so I hope that is an area that
1087 can be considered as well.

1088 We talk also about the safe harbor provisions,
1089 essentially companies that have certain security practices
1090 such as encryption should be encouraged to put in place and
1091 maintain those practices but again we think that notification
1092 can be made to the Federal Trade Commission in those
1093 instances where security breaches occur even it may not be
1094 necessary to notify the target population.

1095 Finally, I would like to point out that since when the

1096 bill was originally introduced there have been significant
1097 changes both in the Internet and also in communications
1098 technology. Facebook, for example, now has 200 million
1099 users. Four years ago when this bill was first considered,
1100 there were many, many fewer people using these social network
1101 services. This has two implications. First of all, there is
1102 a new way to notify people online. It is no longer necessary
1103 to talk just about a website but also a social network
1104 presence. It also means that there is a new risk in data
1105 collection that needs to consider the growing significance of
1106 social network services. And finally, I might mention that
1107 text messaging has become a very effective way to notify
1108 people about things that might concern them regarding
1109 security. We propose in our testimony that where possible,
1110 text messaging be used as a supplement to the other
1111 notification procedures including mail and e-mail.

1112 So thank you again for the chance to testify and I would
1113 be pleased to answer your questions.

1114 [The prepared statement of Mr. Rotenberg follows:]

1115 ***** INSERT 6 *****

|
1116 Mr. {Rush.} The chair now recognizes Mr. Boback for 5
1117 minutes.

|
1118 ^STATEMENT OF ROBERT BOBACK

1119 } Mr. {Boback.} Chairman Rush, Ranking Member Radanovich
1120 and distinguished members of the committee, I thank you for
1121 giving us the opportunity to testify here today.

1122 As many of you discussed in your opening statements the
1123 security risks associated with peer-to-peer, our company,
1124 Tiversa, which I am the CEO of, has unique insight on this in
1125 that Tiversa has the unique technology that allows us to span
1126 out globally to see all information that is occurring on all
1127 the peer-to-peer clients, so it is just a Lime Wire or a
1128 Kazaa or a BearShare, it is everyone, all encompassing, and
1129 we see it in real time. So therefore this provides us a
1130 great insight to provide information to the committee here
1131 today.

1132 This information that we are finding is very sensitive.
1133 There are security measures. I commend the Honorable Ms.
1134 Bono Mack for bringing this here today. The reason why is
1135 that many security professionals around the world in high-
1136 ranking positions in corporations in the United States and
1137 abroad aren't even aware of this, so again, for her insight
1138 to bring this to the committee and bring 1319 forward, it is
1139 very important, because, again, the awareness is still not

1140 where it needs to be. For instance, in the last 60 days,
1141 despite the measures that have been taken by the peer-to-peer
1142 clients, despite which I also admit are improving, Lime Wire
1143 is improving its protocols to decrease the amount of breaches
1144 that have happened, but in the last 60 days Tiversa has
1145 downloaded breaches in the amount of 3,908,000 breaches,
1146 individual breaches in the last 60 days. I find it very
1147 important that 2221 and 1319 are actually discussed on the
1148 same day. The reason why is, this is where breaches are
1149 happening. As Mr. Gingrey of Georgia called out, obviously
1150 we all saw the Wall Street Journal article April 21st about
1151 the Joint Strike fighter. It wasn't reported in the Wall
1152 Street Journal, this was peer-to-peer. The information
1153 unfortunately is still on the peer-to-peer. This was
1154 discovered in January 2005. We discovered it. We reported
1155 it to the DOD. It is still here. It is still out there. It
1156 has never been remediated. Awareness is not where it needs
1157 to be. Oversight is not where it needs to be in order to
1158 address these problems. That is the type of national
1159 security ends.

1160 Now, there are also the consumer ends. From Tiversa, we
1161 process 1.6 billion searches per day every day. Google is
1162 about 170,000 million per day, so we were about nine times
1163 what Google is processing on a daily basis. In those

1164 searches we are able to see what the users are looking for
1165 around the world, and in those searches we see people
1166 searching for your financial records. They are not looking
1167 to apply for a credit card. They are not looking for health
1168 insurance. They are looking for your health insurance
1169 because they want to quickly go online and buy online
1170 pharmaceuticals using your medical insurance card as medical
1171 identity theft. No credit monitoring will stop that. They
1172 want to get your Social Security number filed with your tax
1173 return. We did a study with the Today show showing that in
1174 that instant 275,000 tax returns were found in one search on
1175 the peer-to-peer, so a minimum of 275,000 Social Security
1176 numbers on one time. Now, we have done other searches where
1177 it has been over half a million on one time and yet I would
1178 also strongly urge the FTC that on the website where it would
1179 identify to users that this information is coming from the
1180 peer-to-peer, there is not one mention of peer-to-peer on
1181 where are they getting your information. Nine million
1182 victims every year of identify theft and the number one
1183 mention on the FTC's website is dumpster diving. It doesn't
1184 add up. The numbers don't add up to dumpster diving.
1185 Consumers are not aware of this problem, not from a national
1186 security standpoint. Executives don't know it. Security
1187 executives do not know this problem. Consumers aren't aware

1188 of this problem. They need to know that their information is
1189 out there and it is being sought after on an enormous scale
1190 such that even in our research in the last few months we have
1191 had a 60 percent increase in searches for information that
1192 will lead to identify theft and fraud. This is a serious
1193 growing problem that consumers again are not aware of, so we
1194 applaud 2221 for a national breach. I will tell you that as
1195 we find these breaches, these 3,900,000 breaches, as we can
1196 we return the information and alert the companies to the
1197 breach. Again, we do it out of our duty of care policy.
1198 There are no strings attached to that.

1199 I will tell you that there are thousands of cases that
1200 our employees have provided to users, to companies nationwide
1201 that they completely disregard the breach. Many of those are
1202 actually cited in my written testimony, so you would think
1203 that you are safe if you do not use peer-to-peer. Well, I
1204 will show you in the written testimony there are users out
1205 there that all they did was go to the hospital and they
1206 provided their information there and now that is one of the
1207 things, so individuals need to have an identify theft
1208 protection service as well as a national breach notification
1209 such as 2121, and I thank you for the opportunity and welcome
1210 questions.

1211 [The prepared statement of Mr. Boback follows:]

1212 ***** INSERT 7 *****

|
1213 Mr. {Rush.} Thank you very much. Now the chairman
1214 recognizes Mr. Sydnor. Mr. Sydnor, you are recognized for 5
1215 minutes for opening statement.

|
1216 ^STATEMENT OF THOMAS D. SYDNOR

1217 } Mr. {Sydnor.} Thank you, Chairman Rush, Ranking Member
1218 Radanovich and members of the subcommittee. My name is
1219 Thomas Sydnor and I am a senior fellow at the Progress and
1220 Freedom Foundation. I am here speaking today on my own
1221 behalf, and I am also the author of two studies on the causes
1222 of inadvertent file sharing, File-Sharing Programs and
1223 Technological Features to Induce Users to Share, published by
1224 the United States Patent and Trademark Office, and
1225 Inadvertent File Sharing Revisited, published by the Progress
1226 and Freedom Foundation, and I am here today to testify in
1227 support of H.R. 1319, the Informed Peer-to-Peer User Act.

1228 Mr. {Rush.} Mr. Sydnor, would you please excuse me just
1229 for a moment? I want to alert the members that there is a
1230 little over 5 minutes for a vote, a three-series vote. There
1231 are three votes in the series, and that will be the last
1232 votes of the day. So if members want to leave to go and vote
1233 after this witness completes his opening statement, then the
1234 chair will recess the committee and reconvene at the
1235 conclusion of this series of votes. So we would ask that the
1236 members please return promptly so that we can complete the
1237 questioning of these witnesses and complete this hearing.

1238 Mr. Sydnor, would you please continue?

1239 Mr. {Sydnor.} Thank you, Mr. Chairman.

1240 I am testifying today in support of the bill because my
1241 written statement and my past published work on inadvertent
1242 sharing I think shows that in the past we have tried to rely
1243 on voluntary self-regulation and it has failed. Voluntary
1244 self-regulation should be an incredibly important part of our
1245 technology policy and for that reason it must be taken
1246 seriously. Unfortunately, in the context of distributors of
1247 filing sharing programs used mostly for unlawful purposes, it
1248 has been tried, voluntary self-regulation. It has failed
1249 miserably in the past, and I can report that it is failing
1250 again right now.

1251 I want to consider just as an example the file-sharing
1252 program Lime Wire 5. The DCIA has hailed Lime Wire 5 as the
1253 gold standard for the implementation of its new voluntary
1254 best practices, and Lime Wire itself has a result of this
1255 hearing generated great publicity for itself by telling
1256 Congress that at long last Lime Wire 5 put the final nail in
1257 the coffin of inadvertent sharing of sensitive files, and the
1258 program is that last statement is not even arguably correct,
1259 and to show why, I want you to consider a hypothetical based
1260 upon the recent reports from Today Investigates showing that
1261 in New York State alone researchers could find over 150,000

1262 inadvertently shared tax returns. The report also showed the
1263 real-world consequences of inadvertent sharing by profiling
1264 the Bucci family, who had their tax returns stolen by an
1265 identity thief because they had inadvertently shared their
1266 tax returns because their preteen daughters were using a
1267 file-sharing program reported to be Lime Wire. But the real
1268 problem in such a case is that a tax return is really only
1269 the tip of the iceberg. Such episodes usually occurring mean
1270 that a family is sharing all of its personal data file stored
1271 on the family computer. All the parents' work and personal
1272 documents, scans of legal, medical and financial records,
1273 scanned documents providing identifying information about the
1274 family's children, all of the family's digital photos, all of
1275 its home videos, entire music collection, probably thousands
1276 of files.

1277 Now, consider two families that have been affected by
1278 this type of catastrophic inadvertent file sharing, and just
1279 assume it was caused by an earlier version of Lime Wire.
1280 Consider what happens if they upgrade to Lime Wire 5. One
1281 family doesn't know they have a problem. They are unaware
1282 that a problem exists but they hear reports like Lime Wire 5
1283 has ensured the complete lockdown of the safety and security
1284 of Lime Wire users and so they upgrade to Lime Wire 5. Will
1285 that correct their inadvertent sharing of sensitive documents

1286 problem? It will not. By default, simply by being
1287 installed, the family will continue to share documents that
1288 are by any a reasonable definition sensitive. They will
1289 continue to share the family photo collection. They will
1290 continue to share scanned legal, medical and financial
1291 records, perhaps even tax returns, continue to share data
1292 about their children. They will continue to share all their
1293 home videos. They will continue to share their entire music
1294 collection. So they will continue to be exposed to the full
1295 range of risks: identify theft, data on their children
1296 getting into the hands of the pedophiles that use their
1297 networks, and the risk of a lawsuit.

1298 Now, the other family does know their problem. They
1299 detect it and they resolve it by uninstalling Lime Wire,
1300 remove it from their computer. So this family actually has
1301 put the final nail in the coffin of their inadvertent file-
1302 sharing problem but they hear about Lime Wire, they kids
1303 reinstall it because now it is completely secure. What will
1304 happen? By default, simply by being installed, that program
1305 will revive, will call back from the dead the family's
1306 inadvertent file-sharing problem. It will automatically
1307 begin re-sharing all the data files that were shared before
1308 except for some types simply by being installed. That is not
1309 acceptable behavior, it is not acceptable practice, and I

1310 think it indicates why the committee should be commended for
1311 its work on H.R. 1319. Thank you.

1312 [The prepared statement of Mr. Sydnor follows:]

1313 ***** INSERT 8 *****

|
1314 Mr. {Rush.} The chair thanks this witness and all the
1315 witnesses. Now the chair will ask that this committee stand
1316 in recess until such time as we return from a series of three
1317 votes. I would ask the witnesses if you please would wait so
1318 that the members can come back and ask questions. Thank you
1319 so much. The committee is in recess.

1320 [Recess.]

1321 Mr. {Rush.} The hearing will now come to order. The
1322 chair recognizes himself for 5 minutes for the purposes of
1323 questioning the witnesses.

1324 I would like to start out with some very simple
1325 questions to get on the record how the witness may view the
1326 legislation we are contemplating today. I will ask each and
1327 every one of you if you would just answer with a yes or no if
1328 you can, and if not, give me a very brief explanation of your
1329 answer. So my first question is with regard to H.R. 1319, do
1330 you support the legislation in its current form? If not, do
1331 you support the intent of the bill with revisions? And my
1332 second question, do support H.R. 2221 as it is currently
1333 drafted? If not, do you support the intent of the bill with
1334 some revisions? I will start with Mrs. Harrington.

1335 Ms. {Harrington.} The Federal Trade Commission strongly
1336 supports the intent of both bills. We would like to continue

1337 working with committee staff on revisions to each but we are
1338 very--and we are particularly supportive of the enforcement
1339 authority and tools that both bills give the FTC of civil
1340 penalty authority.

1341 Mr. {Rush.} Thank you.

1342 Mr. Sohn?

1343 Mr. {Sohn.} CDT has significant reservations about H.R.
1344 1319 as drafted but we certainly support the intent. We do
1345 think it may be tricky to figure out the drafting details but
1346 we are certainly happy to work with the committee on that.
1347 On H.R. 2221, we generally do support the bill as drafted.
1348 There are some modifications we have suggested and we
1349 absolutely support the intent.

1350 Mr. {Rush.} Thank you.

1351 Mr. Holleyman?

1352 Mr. {Holleyman.} I actually agree fully with Mr. Sohn's
1353 comment that we support the intent of both bills. We have
1354 some recommendations in our written testimony. I believe
1355 strongly that action is needed. I think it may be more
1356 difficult to make some of the definitions in 1319 but are
1357 certainly eager to work with the committee to ensure the
1358 intent is fulfilled.

1359 Mr. {Rush.} Mr. Lafferty?

1360 Mr. {Lafferty.} I will just speak to 1319. We

1361 absolutely support the intent of the bill, the clear,
1362 conspicuous notice and the informed consent for very
1363 important file-sharing modalities that could have major
1364 impact on consumers. We just don't think it can be
1365 legislated. We have worked hard to try to come up with
1366 suggestions for a redraft and it is very difficult to get the
1367 language not to reach out and touch other kinds of
1368 technologies and future software applications that would be
1369 impacted and disadvantage U.S. firms from overseas
1370 competitors. So we support the intent but not the language.

1371 Mr. {Rush.} Mr. Pratt?

1372 Mr. {Pratt.} The CDIA has no position on H.R. 1319.
1373 With regard to H.R. 2221, we certainly support the intent.
1374 We have outlined in our written testimony the range of
1375 suggestions about how we could align the bills with other
1376 federal laws and if we could accomplish that goal, I think we
1377 would feel more comfortable with the final work product.
1378 Thank you.

1379 Mr. {Rush.} Thank you.

1380 Mr. {Rotenberg.} Mr. Chairman, we do support the intent
1381 of H.R. 2221 and generally support the legislation as
1382 drafted. We have a number of suggestions in our testimony
1383 for how to strengthen it.

1384 With respect to 1319, we don't have a position for or

1385 against the bill. With respect to the intent behind 1319, we
1386 think it may be possible to get to some of the concerns
1387 regarding security through other legislation but we would
1388 certainly be happy to work with the committee to see how it
1389 can be accomplished.

1390 Mr. {Rush.} Mr. Boback?

1391 Mr. {Boback.} Mr. Chairman, we strongly support both
1392 2221 as well as 1319 in clearly raising awareness and
1393 providing some responsibility and structure to a very needed
1394 process both on the peer-to-peer as well as just federal data
1395 breach notification.

1396 Mr. {Sydnor.} Mr. Chairman, I will confine my comments
1397 to H.R. 1319. Yes, absolutely strongly support the intent of
1398 the bill. I am aware that there are legitimate concerns
1399 about making sure that we don't necessarily sweep in
1400 entirely--potentially entirely legitimate uses of peer-to-
1401 peer technology and would be happy to continue to work with
1402 the committee and anyone else to try to get to a place where
1403 everyone is comfortable.

1404 Mr. {Rush.} The chair thanks the witnesses. The
1405 chair's time is concluded. The chair now recognizes Ms. Bono
1406 Mack from California for 5 minutes for questioning.

1407 Ms. {Bono Mack.} I thank the chairman and our panelists
1408 also for your time today.

1409 Mr. Lafferty, I would like to read to you a bolded
1410 warning in the user guide on the Lime Wire website entitled
1411 ``Using Lime Wire and P2P software safely.'' The warning
1412 states, and I quote, ``Please ensure that any folder on your
1413 computer that contains personal information is not included
1414 in your Lime Wire library.'' So tell me, Mr. Lafferty, if I
1415 were to complete a default installation of Lime Wire 5.1.2,
1416 what files and folders will the mere installation of the
1417 program included in my Lime Wire library?

1418 Mr. {Lafferty.} With Lime Wire 5 and later versions of
1419 Lime Wire, sensitive file types, which are a large number of
1420 extensions of files to protect your spreadsheets, your Word
1421 documents, PDFs, things that might have sensitive data, are
1422 unshared by default. So I would completely refute the
1423 testimony of Tom Sydnor earlier. It just isn't true. When
1424 you--neither example that he gave with the family that kept--
1425 just upgraded the version or the one that uninstalled it and
1426 reinstalled it, in both cases all the sensitive file types
1427 are unshared by default. It is over. They are no longer
1428 accessed or shared. To re-share any of those files, you
1429 would have to individually take the file and go through--
1430 ignore several warnings to put those individual files into
1431 the mode where they could be shared and then be asked whether
1432 you want to share that with specific friends or the network

1433 at large. So Lime Wire 5 has done away with the concept of
1434 shared folders really and now it is a file-by-file--

1435 Ms. {Bono Mack.} There are specific warnings? What do
1436 they say? And it is not--it is still actually sort of an
1437 inherent default. You have little boxes that come up. I
1438 believe there are four different boxes that are there. And
1439 one does say my documents, so you just that that could be an
1440 Excel spreadsheet which in fact would probably be saved under
1441 a my documents folder, would it not?

1442 Mr. {Lafferty.} If you chose to put the my documents
1443 folder into a shared mode, it would still--

1444 Ms. {Bono Mack.} Is that the default for an Excel
1445 spreadsheet for the standard user?

1446 Mr. {Lafferty.} I don't understand the question.

1447 Ms. {Bono Mack.} Where is a default Excel spreadsheet
1448 saved on your computer, on your hard drive? Is it not
1449 necessarily defaulted to my documents?

1450 Mr. {Lafferty.} It is probably different for every
1451 person, but the point is--

1452 Ms. {Bono Mack.} Probably different? What is the
1453 default? Where does--Mr. Sydnor, perhaps you have the answer
1454 to that.

1455 Mr. {Lafferty.} It doesn't really matter where it is
1456 that. That file type won't be shared.

1457 Ms. {Bono Mack.} How could it not matter? With all due
1458 respect, how could it not matter where it is? That is the
1459 root of the whole problem here.

1460 Mr. {Lafferty.} Because it won't be shared.

1461 Ms. {Bono Mack.} Unless you check simply one of the
1462 four--

1463 Mr. {Lafferty.} Unless you choose that individual file
1464 if it has that Excel spreadsheet.

1465 Ms. {Bono Mack.} That individual file?

1466 Mr. {Lafferty.} Individual file, correct.

1467 Ms. {Bono Mack.} Mr. Sydnor, do you care to comment on
1468 that?

1469 Mr. {Sydnor.} Yes. That is not quite an accurate
1470 statement about how the Lime Wire my library feature works.
1471 My library in Lime Wire 5 basically are the set documents
1472 that are going to be managed in Lime Wire and thereby that
1473 set of documents is going to be much easier to share because
1474 they are going to be in the library and there will be a
1475 button to click to share them, and that is why Lime Wire
1476 users' guide has the warning that you read, please ensure
1477 that any folder in your computer that contains personal
1478 information is not included in your Lime Wire library. Now,
1479 by default when you install Lime Wire 5.1, and I did it last
1480 night again, the default option is to have Lime Wire put all

1481 the files stored in your my documents folder and all of its
1482 subfolders into the Lime Wire library. That alone will not
1483 share them but it will make them available for sharing and
1484 much easier to share and therefore the behavior of the
1485 program simply not consistent with the advice in the users'
1486 guide. As to my testimony earlier, it was quite correct.
1487 The difference--the reason I think we are getting confused
1488 is, when I say sensitive files, I mean files that would
1489 actually be sensitive to share over a network like Gnutella
1490 so you have, for example, scans of your family medical
1491 records and tax returns, those can be stored in image file
1492 formats often and those will be shared by default, and if you
1493 upgrade to Lime Wire 5, it will continue to share those file
1494 types if you were sharing them before, and if you install
1495 Lime Wire 5 on your computer and a previous version of Lime
1496 Wire has ever been there, then it will automatically begin
1497 re-sharing files that were shared previously. So simply
1498 installing the program can indeed resume sharing of files
1499 even if you are installing on a computer where there is no
1500 version of Lime Wire currently installed. I am correct about
1501 that. I reran the test again this morning before the
1502 hearing.

1503 Ms. {Bono Mack.} Thank you. I know my time is expired
1504 and I hope we have a second round. Thank you, Mr. Chairman.

1505 Mr. {Rush.} The chair intends to have a second round.
1506 The chair now recognizes the gentleman from Georgia, Mr.
1507 Barrow, for 5 minutes.

1508 Mr. {Barrow.} I thank the chair. I want to try and get
1509 my arms around the inadequacy of the current situation and
1510 talk about what it is this legislation proposes to do in
1511 order to try and alter the situation for the better.

1512 Ms. Harrington, am I correct in understanding that there
1513 are very limited tools available to the FTC right now to deal
1514 with this issue, that basically the only option you have
1515 under current law is to initiate a specific enforcement
1516 action against somebody, a fact-specific action based on a
1517 specific instance and that basically you are pretty much
1518 limited to, is it adjunctive proceedings? Is that about the
1519 extent of it?

1520 Ms. {Harrington.} That is right.

1521 Mr. {Barrow.} No civil penalties whatsoever?

1522 Ms. {Harrington.} No civil penalties.

1523 Mr. {Barrow.} No rulemaking authority, no prescribing
1524 of proper procedures or best practices, you just have to go
1525 after individual cases and all you can do is tell folks to
1526 stop doing what they are doing when you prove that they have
1527 done it?

1528 Ms. {Harrington.} The rulemaking authority available to

1529 the Commission is under the Magnusson-Moss amendments to the
1530 FTC Act and those are laborious and take a very long time,
1531 the procedures to use.

1532 Mr. {Barrow.} So what we are proposing to give the FTC
1533 under 1319 would give you all some authority you don't have
1534 right now. Are the civil penalties helpful to you all in
1535 trying to bring some order to this situation?

1536 Ms. {Harrington.} There are two things that are
1537 helpful. Civil penalty authority is very helpful, and also
1538 to the extent that some practices in these very fact-specific
1539 situations might be injurious but neither deceptive nor
1540 unfair, then having additional statutory authority is very
1541 helpful.

1542 Mr. {Barrow.} Earlier on in the testimony, we heard
1543 some folks raise some issues about the international end of
1544 things. We all know we are connected to a worldwide web and
1545 that any effective regulation of this marketplace in our
1546 country is going to involve dealings with folks who can cross
1547 the boundaries in cyberspace pretty much at will. What was
1548 your concern, if not the extraterritoriality of the law, the
1549 extraterritorial effect of us being able to regulate this?
1550 How do you think we can address that supposed shortcoming of
1551 us attempting to regulate this on our own shores?

1552 Ms. {Harrington.} Well, first of all, the subcommittee

1553 was instrumental in giving the Commission additional
1554 authority under the U.S. Safe Web Act, which we used to get
1555 information about overseas targets and to enlist help from
1556 other governments and that is very useful. But that said, if
1557 there are overseas software providers who are making
1558 available file-sharing software that is injurious to U.S.
1559 consumers, we can certainly assert our jurisdiction over
1560 those practices that occur within the United States but we
1561 may not be able to reach the purveyors if they are in other
1562 countries and particularly in countries that aren't
1563 particularly interested in helping out.

1564 One of the things that we are very concerned about is
1565 that the dominant players in this industry, which are in the
1566 United States, do the best thing and the right thing and we
1567 think that setting some legislative standards such as the
1568 ones that are set forth in the bill would really help. We
1569 want the U.S. players to be the best players so that they
1570 continue to be the dominant players and the ones that
1571 consumers can use with some confidence.

1572 Mr. {Barrow.} The impression I get from what you are
1573 saying, this is how I hear what you are saying, is that if we
1574 police the marketplace where everybody shops, we don't have
1575 to worry about the marketplace where few very people shop or
1576 hardly anybody goes. Is that a fair way of putting it?

1577 Ms. {Harrington.} Well, we certainly should police the
1578 marketplace where everybody stops if that marketplace is
1579 subject to our jurisdiction.

1580 Mr. {Barrow.} But the high-volume users, the ones that
1581 have the lion's share of the market, if we can make sure that
1582 what they are doing is right and appropriate and folks who
1583 trade at these places will not have to worry about losing
1584 their stuff, we don't have to worry quite so much about those
1585 areas that might be hard to reach. Why strain at a gnat and
1586 swallow an elephant in the process.

1587 Ms. {Harrington.} You know, that is certainly the
1588 intention. There is always a risk that overseas operators
1589 can gain in market share in the United States by doing--you
1590 know, by gaining some sort of competitive advantage over the
1591 regulated entities in our marketplace but, you know, that is
1592 not a worry right now that is keeping me awake at night.

1593 Mr. {Barrow.} I will wait for a second round, Mr.
1594 Chairman. Thank you, ma'am.

1595 Mr. {Rush.} Thank you.

1596 The chair now recognizes the gentleman from Louisiana,
1597 Mr. Scalise, for 5 minutes.

1598 Mr. {Scalise.} Thank you, Mr. Chairman. Really I can
1599 open this up to the whole panel on H.R. 1319. Do you think
1600 this will help prevent a legal use of peer-to-peer software

1601 including stealing personal records, copyright violations and
1602 things like sharing child pornography?

1603 Ms. {Harrington.} I think it will help under some
1604 circumstances and under others we need more. The data
1605 security bill actually could be very helpful here too
1606 because, as I mentioned in my oral statement, there are
1607 really three scenarios where sensitive information is shared.
1608 One is when consumers don't know, don't understand, and this
1609 bill will hopefully go a long way I think there. It is not
1610 going to help when the problem is malware, and it is not
1611 going to help when the problem is a business that has not
1612 prohibited and barred from its system and its computers file-
1613 sharing software and it is not going to help if the problem
1614 is that an employee of a company takes sensitive information
1615 home and puts it on his or her computer and that computer has
1616 file-sharing software or malware on it that extracts that, so
1617 it is going to go a long way to help in scenario one.

1618 Mr. {Scalise.} Anybody else want to touch on that?

1619 Mr. {Sohn.} I will just say I do think the intent and
1620 the focus of the bill is certainly on the inadvertent
1621 disclosure so that the privacy-related concerns, I think that
1622 would be the main impact and is the main thrust of the bill.

1623 Mr. {Scalise.} Let me ask about the data breaches that
1624 have occurred, I think FTC had dealt with it, the largest one

1625 I have seen, the TJX, which I think initial estimates were
1626 about 45 million Visa/MasterCard records were breached.
1627 Ultimately it turned out somewhere close to 100 million were
1628 breached, and you all had brought charges against them, and
1629 subsequently other companies. Is there now an industry
1630 standard for data protection? What is your feeling on where
1631 we are today versus some of those cases a few years ago?

1632 Ms. {Harrington.} Well, there are certainly well-
1633 established good practices that in the cases that we have
1634 brought were not followed. For example, you know,
1635 downloading available patches, preventing against well-known
1636 attacks and kinds of attacks are well-settled, you know,
1637 necessary practices. They are not even best practices. They
1638 are necessary. And those companies did not follow those
1639 practices.

1640 Mr. {Scalise.} Anybody else want to add anything to
1641 that? We are getting into now an area of moving towards
1642 electronic medical records. There was some funding language
1643 in the stimulus bill to start going down that road more as
1644 people's health information gets put on the Web more and
1645 more. What kind of protections are there today, what kind do
1646 we need, whether it is in either these two bills or another
1647 vehicle to protect people's health records as they become
1648 available on the Internet so that they are only available to

1649 the doctors who need to be reviewing them?

1650 Ms. {Harrington.} Well, the Recovery Act also directed
1651 both the FTC and the Department of Health and Human Services
1652 to do rulemaking to set standards for breach notification
1653 when consumers' sensitive health information is placed at
1654 risk. The FTC, as I mentioned, has just issued a proposed
1655 rule dealing with personal health records and other non-
1656 HIPAA-covered entities that may have this sensitive
1657 information to set breach notification standards and we are
1658 continuing also to work with HHS to do a report that is due
1659 back to Congress in a year on these issues.

1660 Mr. {Scalise.} Any of you all doing any work on that
1661 issue? Mr. Boback?

1662 Mr. {Boback.} I would like to also comment on that.
1663 There are no standards as far as peer-to-peer notifications.
1664 There are no standards as far as peer-to-peer security
1665 measures. In fact, most companies don't even have any
1666 standards on peer-to-peer. When asked, most corporations,
1667 large and scale, what information they are doing about peer-
1668 to-peer, most people, if they respond at all will say that
1669 they are blocking peer-to-peer and that they have a policy
1670 against it. That is the extent of it. And I will tell you
1671 that--or they will say that they have a firewall or an
1672 encryption of which nothing--firewall does not stop peer-to-

1673 peer, encryption does not stop peer-to-peer. Intrusion
1674 prevention detection and all the standard security measures
1675 do not peer-to-peer disclosures from happening, which is why
1676 in the past 60 days we have had, you know, almost 4 million
1677 disclosures of this type via peer-to-peer because there is
1678 just no standards.

1679 Mr. {Scalise.} And finally Mr. Holleyman.

1680 Mr. {Holleyman.} Mr. Scalise, we believe that the
1681 incentives that are in Chairman Rush's bill that would
1682 encourage a marketplace to grow for companies who hold
1683 sensitive data to use proper security technologies to make
1684 that information inaccessible to anyone who might actually
1685 breach it, that those market-based incentives is a great
1686 supplement to the enforcement authority that the bill would
1687 give. So we think the two together can be effective.

1688 Mr. {Scalise.} Thanks. I yield back, Mr. Chairman.

1689 Mr. {Rush.} The chair intends to engage the members of
1690 the committee in a second round of questioning and we will
1691 allow each member an additional 2 minutes for the second
1692 round of questioning. The chair recognizes himself now for
1693 the second round and allocates 2 minutes for the purposes of
1694 questioning.

1695 Mr. Rotenberg and Mr. Sohn, is the definition of
1696 personal information under H.R. 2221, is it adequate in terms

1697 of data security? The bill only addresses financial
1698 information. Should we also consider requiring companies to
1699 secure sensitive information such as medical information or
1700 password numbers or et cetera? I mean, should we expand the
1701 definition of personal information?

1702 Mr. {Sohn.} Well, the bill has several different
1703 components, and I think for purposes of the breach
1704 notification component, the definition there is fairly close
1705 to what has been done in a lot of the States and it reflects
1706 a lot of what has been common in the data breach notification
1707 area. I think for purposes of something like security
1708 standards, asking companies to have reasonable procedures in
1709 place to protect data, there is no reason to restrict it to
1710 the rather narrow set of data that is in the definition of
1711 personal information now because what is currently in the
1712 bill only applies--it is not just name and address and some
1713 other information. There actually has to be either a Social
1714 Security number or a financial account number plus password
1715 or a driver's license number, something like that. So I do
1716 think that the bill might consider using a broader definition
1717 of personal information for some purposes and the narrower
1718 definition for others.

1719 Mr. {Rotenberg.} Mr. Chairman, in my written statement
1720 I made a suggestion on this issue of personal information. I

1721 do think it is appropriate to have a broader standard and
1722 also to recognize that some of the personal identifiers
1723 nowadays aren't just limited, for example, to a Social
1724 Security number or driver's license number. There are other
1725 types of personal identifiers like a Facebook member number
1726 or even the IP address associated with your computer that
1727 needs to be incorporated as well. So I think those changes
1728 can be made both to get to more circumstances where the bill
1729 should reach and also new types of identifiers.

1730 Mr. {Rush.} The chair thanks the witnesses. Now the
1731 chair recognizes the gentlelady from California for 2 minutes
1732 for additional questions.

1733 Ms. {Bono Mack.} I thank the chair for the second
1734 round.

1735 Mr. Holleyman, you testified that the P2P bill would
1736 cover more than just the illegitimate purpose software. You
1737 identified a number of legitimate uses of P2P software such
1738 as bicoastal collaboration on projects. I think you actually
1739 mentioned Palm Springs to Chicago airports collaborating. So
1740 this is of course when used correctly beneficial use of P2P
1741 software. So we all agree that this technology can be
1742 extremely helpful but if such programs are covered by H.R.
1743 1319, what is the harm? How is notice and consent an issue?
1744 Back to the Palm Springs-Chicago, yes, I can see them

1745 collaborating on plans but I don't think they necessarily
1746 want to collaborate on payroll numbers and the like. So how
1747 is notice and consent an issue in this case?

1748 Mr. {Holleyman.} Ms. Bono Mack, our sense is that there
1749 is a rapid growth in the legitimate uses of P2P, and that it
1750 will become a de facto part of how we use technology that
1751 most people will want to use. So our sense is as that part
1752 of the market grows, we want to ensure that the legislation
1753 doesn't overreach to get into things which all of us would
1754 generally agree would not necessarily need--an initial notice
1755 that that is there is fine but the process of how you would
1756 then disable that needs to be clarified.

1757 Ms. {Bono Mack.} Which is growing faster, illegitimate
1758 or legitimate uses?

1759 Mr. {Holleyman.} I think our sense as technologists is--
1760 -and I am not a technologist, I play one on TV, but not as
1761 technologists but our engineers and our companies believe
1762 that legitimate purposes of peer-to-peer in the next 10 years
1763 will certainly grow much faster than the illegitimate ones.

1764 Ms. {Bono Mack.} In the next 10 years, quickly in 10
1765 seconds, Mr. Boback, which has grown faster, legitimate or
1766 illegitimate uses?

1767 Mr. {Boback.} I will tell you that legitimate uses are
1768 now emerging so while there is still a growth at this point

1769 because the awareness is still decreased and there is not
1770 enough awareness as to the problem, the legitimate uses and
1771 the distribution content is an absolute must going forward.
1772 So I am a supporter of peer-to-peer, however, the security
1773 measures just as in the early stages of the World Wide Web
1774 need to be addressed as in your bill 1319.

1775 Ms. {Bono Mack.} Thank you.

1776 Mr. {Rush.} The chair now recognizes the gentleman from
1777 Georgia.

1778 Mr. {Barrow.} I thank the chair. I think Ms. Bono Mack
1779 is getting to the heart of the issue on the peer-to-peer
1780 legislation. If I could reframe the issue, we want to fix
1781 what is broke with this system. There is stuff out there
1782 that is inside this legislation's definition of peer-to-peer
1783 file-sharing program that is malicious. There is stuff out
1784 there that is inside this definition that is perfectly
1785 benign.

1786 Mr. Holleyman and Mr. Sohn, I am going to pitch this one
1787 in you all's direction. How would you all define what we are
1788 getting at in such a way as to stop the bad stuff and allow
1789 all the other stuff to continue without having to have a
1790 proliferation of warnings and opt-outs that basically hobble
1791 this technology before it can even get started? Take a shot
1792 at how you would define this in order to be able to reach the

1793 stuff you want to reach.

1794 Mr. {Holleyman.} I will start on that, Mr. Barrow. In
1795 our testimony, we have actually listed five ways in which we
1796 would modify the definition in the bill and believe that if
1797 those types of changes are made, that that would be useful
1798 and would help preserve the intent of the bill including
1799 looking at the type of purposes that peer-to-peer file-
1800 sharing program is typically used for, going at many of those
1801 things like copyright infringements, which are a huge source
1802 of concern to--

1803 Mr. {Barrow.} Is that an effective way of defining it
1804 though so that the regulators can get at what is going on?

1805 Mr. {Holleyman.} We actually think that the regulators
1806 would--their hand would be strengthened by more precision in
1807 the definition rather than the breadth that is in there
1808 currently.

1809 Mr. {Barrow.} Mr. Sohn, what do you think?

1810 Mr. {Sohn.} I also set forth in my testimony some ideas
1811 on that point of how you might make this more narrow and
1812 apply to what we think of as file-sharing software. I agree
1813 with Mr. Lafferty's testimony that the key here really isn't
1814 peer-to-peer. Peer-to-peer is a kind of architecture. It is
1815 really about file-sharing functions that could enable
1816 documents and other kinds of files on a user's local computer

1817 to be made available to third parties, you know, in bulk and
1818 third parties that haven't been selected or aren't even known
1819 to the user and so we propose four bullet points of items
1820 that we think could be in the definition but it tends to
1821 focus on that, the ability to share files with unknown
1822 parties with no intervening action or knowledge or selection
1823 by the user in terms of who that file will be shared with.

1824 Mr. {Barrow.} Mr. Chairman, my time is expired but I
1825 would like to ask the witnesses to go beyond that and
1826 actually be prepared to work with counsel and us to see if we
1827 can actually come up with some concrete language to
1828 accomplish this. Thank you. I yield the mic.

1829 Mr. {Rush.} The chair now recognizes the gentleman from
1830 Louisiana for an additional 2 minutes.

1831 Mr. {Scalise.} Thank you again, Mr. Chairman.

1832 These two bills might not necessarily be the vehicles
1833 for it but they might. It has been a problem for years,
1834 especially with identify theft getting worse with so many
1835 documents and authenticators that use Social Security numbers
1836 that require Social Security numbers to be used or documents
1837 that are public record that still require people to use
1838 Social Security numbers. A number of States have gone on
1839 their own and tried to ferret those out and prohibit Social
1840 Security numbers on public documents but it is not universal.

1841 There is no real standard still. I think there as standalone
1842 legislation, it might have been in the last Congress, that
1843 really didn't go anywhere but there is a way that we can have
1844 some kind of standard to protect people's Social Security
1845 numbers so that they are not required for certain documents
1846 or authenticators so that they are not so easily obtainable
1847 by third parties that are trying to take them for bad
1848 purposes? I will start it off with Ms. Harrington and
1849 anybody else that wants to take a shot.

1850 Ms. {Harrington.} Well, as part of the President's
1851 identify theft task force work that we have been engaged in,
1852 there are couple of important initiatives that we are
1853 supporting. One, the task force brought about a government-
1854 wide examination of government uses of Social Security
1855 numbers with the goal of minimizing to circumstances where
1856 the number is absolutely essential, federal government
1857 agencies' use of Social Security numbers, and I think a lot
1858 of progress has been made in the government on that. Number
1859 two, the FTC as part of the identify theft task force work
1860 convened a workshop and has continued to work on the question
1861 of authentication and how better authentication procedures
1862 and technologies can be developed so that something like the
1863 ubiquitous Social Security number is no longer needed. But
1864 there are lots of commercial settings right now where both

1865 consumers and businesses benefit from the use of Social
1866 Security numbers and may need them, and until we have much
1867 better authentication measures available, it is a very tough
1868 question to answer what to use instead of Social Security
1869 numbers. For example, consumers have really benefited in
1870 many instances from being able to quickly get a loan to get a
1871 car. That whole credit reporting system depends on Social
1872 Security numbers, and you know, we need a replacement but we
1873 don't have one yet.

1874 Mr. {Scalise.} And at least in the government sector
1875 where we can set up a mechanism where people aren't required
1876 to have it on a document that is public record because--

1877 Ms. {Harrington.} Right.

1878 Mr. {Scalise.} --clearly in the government arena, there
1879 are records that are public and some of those records require
1880 a Social Security number, which obviously poses big, big
1881 security breach problems that have been documented. In this
1882 legislation, if there a way to maybe try to address that, I
1883 don't want to interfere with the chairman or Ms. Bono Mack's
1884 bill but if there is a way we can do something that doesn't
1885 necessarily cause other problems on the other side we can try
1886 to address a narrow part of that problem.

1887 Mr. {Rush.} The gentleman's time is expired.

1888 Mr. {Scalise.} Thank you.

1889 Mr. {Rush.} The chair really just wants to again thank
1890 the witnesses. We have imposed on your time pretty
1891 significantly this afternoon and we certainly are
1892 appreciative of the fact that you have allowed us to do that
1893 and you have been a great panel. If you would be so kind, we
1894 want to keep the record open for at least 72 hours until
1895 there might be members of the subcommittee who will in
1896 writing ask questions and if you would respond in writing
1897 within 72 hours, the chair would certainly appreciate that.

1898 So thank you so very much again and you have really done
1899 this subcommittee quite a great service. The hearing now
1900 stands adjourned.

1901 [Whereupon, at 4:45 p.m., the subcommittee was
1902 adjourned.]