

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 HIF113.160

3 HEARING ON ``COMMUNICATIONS NETWORKS AND CONSUMER PRIVACY:

4 RECENT DEVELOPMENTS''

5 THURSDAY, APRIL 23, 2009

6 House of Representatives,

7 Subcommittee on Communications, Technology and the Internet

8 Committee on Energy and Commerce

9 Washington, D.C.

10 The subcommittee met, pursuant to call, at 10:05 a.m.,
11 in Room 2322 of the Rayburn House Office Building, Hon. Rick
12 Boucher (chairman) presiding.

13 Members present: Representatives Boucher, Rush, Eshoo,
14 Stupak, DeGette, Weiner, Christensen, Castor, Space, Stearns,
15 Shimkus, Buyer, Radanovich, Bono Mack, Terry, and Blackburn.

16 Staff present: Roger Sherman, Chief Counsel; Tim
17 Powderly, Counsel; Shawn Chang, Counsel; Greg Guice, Counsel;
18 Amy Levine, Counsel, Sarah Fisher, Special Assistant; Pat

19 Delgado, Chief of Staff Congressman Waxman; Neil Fried,
20 Counsel; and Sam Costello, Legislative Clerk.

|

21 Mr. {Boucher.} The subcommittee will come to order.
22 Broadband networks are a primary driver of the national
23 economy and it is fundamentally in the Nation's interest to
24 encourage their expanded use. One clear way Congress can
25 promote a greater use of the Internet for a variety of
26 purposes including access to information, electronic commerce
27 and entertainment is to assure Internet users of a higher
28 degree of privacy protection with regard to data that is
29 collected concerning their Internet usage. It is my
30 intention for the subcommittee this year to develop on a
31 bipartisan basis legislation extending to Internet users that
32 assurance that their online experience is more secure. We
33 see this measure as a driver of greater levels of Internet
34 uses such as electronic commerce. Not as a hindrance to
35 them.

36 Today's discussion is the first of two presently planned
37 hearings relating to consumer privacy on electronic networks.
38 Today we explore network-based privacy matters including the
39 growing deployment of deep packet inspection technologies and
40 location-based privacy enabled by specific technologies.
41 There are additional privacy related matters that we intend
42 to explore including targeted and behavioral advertising.
43 And we are now planning to conduct a joint hearing with the

44 full committee's Subcommittee on Commerce, Trade and Consumer
45 Protection during the early period of the summer in order to
46 examine online privacy including behavioral advertising at
47 which Internet-based companies will be invited to testify
48 before the subcommittee.

49 A range of concerns related to online advertising should
50 be vetted and just as there are concerns about the privacy
51 implications of the network-based technologies upon which we
52 are focusing this morning. Those online advertising concerns
53 will be thoroughly vetted at the joint hearing we will have
54 with the other subcommittee this summer. But today's focus
55 is on emerging network technologies that have significant
56 privacy implications and three of them will be highlighted by
57 witnesses testifying to us today.

58 Deep packet inspection enables the opening of the
59 packets which actually hold the content of Internet
60 transported communications. Through the use of DPI, the
61 content can be fully revealed and fully examined. It has
62 generally been accepted that there are beneficial uses for
63 DPI, such as enabling better control of networks and the
64 blocking of Internet viruses and worms.

65 DPI also enables better compliance by Internet service
66 providers with warrants authorizing electronic message
67 intercepts by law enforcement, but its privacy intrusion

68 potential is nothing short of frightening. The thought that
69 a network operator could track a users every move on the
70 Internet, record the details of every search and read every
71 e-mail or document attached to an e-mail message is alarming.
72 And while I am certain that no one appearing on the panel
73 today uses DPI in this manner, our discussion today of the
74 capabilities of the technology and the extent of its current
75 deployment, any projection that could be made about its
76 anticipated schedule and path of deployment and the uses to
77 which that technology is currently being put will give us as
78 a subcommittee a better understanding of where to draw the
79 lines between permissible and impermissible uses, or uses
80 that might justify opt-in as opposed to opt-out consent from
81 Internet users.

82 I look forward to hearing from our witnesses this
83 morning about how we can best balance the deployment of DPI
84 with adequate protection for consumers' privacy. For
85 example, should a network operator's use of DPI always
86 require opt-in consent or is opt-out sometimes appropriate
87 and if so, under what circumstances would opt-out be
88 appropriate? What services that consumers consider essential
89 to the safe and effective functioning of the Internet are
90 advanced through deep packet inspection?

91 Since the death of NebuAd, DPI-based behavioral

92 advertising service last year, do we now see other companies
93 using DPI in order to deliver behavioral advertising? What
94 if any safeguards are in place to ensure that consumers are
95 giving meaningful consent to the tracking of their activities
96 on the Internet? These and other questions deserve our
97 consideration this morning.

98 I also look forward to learning about other emerging
99 network-based technologies such as Project Canoe on the cable
100 platform and Loopt and the wireless-base employing new uses
101 of cable set top boxes and GPS tracking capabilities on
102 wireless devices. What benefits do these services offer to
103 consumers and how should the network operator procure
104 meaningful consent from users for their use?

105 We are also interested in hearing a preview of what the
106 future of network-based technologies may hold. What new
107 services may they enable and how do we accommodate with
108 regard to them key privacy concerns? So I look forward to
109 hearing from our distinguished panel and I want to thank each
110 of our witnesses for appearing here this morning and sharing
111 their expertise and views with the subcommittee.

112 [The prepared statement of Mr. Boucher follows:]

113 ***** COMMITTEE INSERT *****

|
114 Mr. {Boucher.} At this time, I am pleased to recognize
115 the Ranking Republican Member of the subcommittee, the
116 gentleman from Florida, Mr. Stearns.

117 Mr. {Stearns.} Good morning and thank you, Mr.
118 Chairman, and I appreciate your opening statement and you are
119 offering a bipartisan tone to it, and your interest in having
120 additional hearings including with the Commerce, Consumer
121 Protection Trade which I chaired during Republican majority.

122 Our goal today should be to broadly examine how
123 companies are using consumer Internet behavior to tailor
124 online advertising, both the benefits to the consumers as
125 well as any potential concerns that have not already been
126 addressed by industry. Our focus should go beyond only
127 broadband providers and also look at the entire Internet
128 universe, including search engines and Internet advertising
129 networks. We cannot have this discussion without addressing
130 them, as well.

131 Whatever the appropriate standards are, they should
132 apply to everyone. We need to be consistent. Consumers
133 don't care if you are a search engine or a broadband
134 provider. They just want to ensure that their privacy is
135 protected.

136 I hope, Mr. Chairman, you will agree to hold more

137 privacy hearings on this subcommittee and I am glad to hear
138 that you will so that we hear from the network operators.
139 That is the only way members can be fully informed about
140 these issues before marking up any legislation.

141 As we move forward towards privacy legislation we must
142 empower consumers to make their own privacy-related
143 decisions. Only the consumer knows how he or she feels about
144 the information that is being collected, the parties doing
145 the collecting and the actual purpose for which the
146 information will ultimately be used. Congress cannot and
147 should not make that decision for them. We need to place the
148 control over consumer information with the consumer himself.
149 This means companies should be as transparent as possible
150 about what information they collect and how do they use this
151 information, that way consumers will be better able to make
152 informed privacy decisions.

153 We also need to examine the ways in which the use of
154 behavioral information for marketing has been shown to have
155 already harmed consumers. It is imperative that there be
156 some evidence of harm if we are going to regulate this
157 practice or we run the risk of prematurely restricting the
158 latest technological advancement related to online marketing.

159 Consumers' online activities provide advertisers with
160 valuable platforms upon which to market their products, their

161 services. Collecting this type of information for targeted
162 advertising is very important because it allows many of these
163 products and services to remain free to consumers. Without
164 this information, websites would either have to cut back on
165 their free information and services or would have to start
166 charging a fee to see to consumers. Neither result is good.
167 Over-reaching privacy regulations, particularly in the
168 absence of consumer harm, could have a significant negative
169 economic impact at a time while many businesses in our
170 economy are struggling. So let us look very closely at these
171 issues before we leap to legislative proposals.

172 We also need a consumer-based approach. Consumers are
173 the best judges. We will not truly address the privacy
174 implications of tailored Internet advertising unless we shift
175 the discussion towards consumer-centric approaches and away
176 from the characteristics of the companies, like the
177 particular technology they use or their corporate structure
178 itself. Whatever we do, we must apply the same standards of
179 privacy to companies collecting this type of information for
180 the same type of purposes, whether it is a phone company, a
181 cable company or companies like Google, Yahoo or Microsoft.
182 Consumers don't care how their privacy has been invaded.
183 What they care about is what the information is that is
184 collected and how it is being used.

185 Now, Mr. Chairman, as you have mentioned, I have had a
186 record of privacy when I was chairman of the trade and
187 consumer protection subcommittee. We held the most extensive
188 hearings on the topic of privacy and following these hearings
189 I offered and introduced the Consumer Privacy Protection Act,
190 which I hope will be used as a baseline for new legislation.
191 This bill would have required data-collectors to provide
192 consumers with information on the entity collecting the
193 information and the purposes for which the information was
194 being collected.

195 Furthermore, in 2005 I held two hearings on identity
196 theft and security breaches involving personal information.
197 These hearings led me to introduce the Data Accountability
198 and Trust Act which would have required any entity that
199 experiences a breach of security such as a business to notify
200 all those in the United States whose information was acquired
201 by an unauthorized person as a result of that breach.

202 So, Mr. Chairman, I look forward to our hearings.
203 Protecting consumers' privacy is a very serious issue and one
204 that needs to be fully examined and I think your leadership
205 on this is to be commended and I look forward to continuing
206 our work together.

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

208 ***** COMMITTEE INSERT *****

|

209 Mr. {Boucher.} Well, thank you very much, Mr. Stearns,
210 and let me simply briefly respond by saying that I appreciate
211 and agree with your suggestions for the focus of our future
212 hearing or hearings on this very important set of privacy
213 concerns. And I want to acknowledge the gentleman's
214 leadership in sponsoring comprehensive and thoughtful
215 legislation in previous Congresses relating to privacy. I
216 was pleased at that time to be the lead Democratic cosponsor
217 of the gentleman's bill. And will be, well, I couldn't
218 resist noting that, and we will be relying on the gentleman's
219 experience and expertise on this subject as we construct
220 bipartisan privacy legislation in this Congress.

221 The gentlelady from California, Ms. Eshoo, is recognized
222 for 2 minutes.

223 Ms. {Eshoo.} Thank you, Mr. Chairman, for holding this
224 hearing on network privacy.

225 As a member of the House Intelligence Committee, I
226 understand that the most valuable intelligence is to know how
227 someone thinks because that enables one to predict what they
228 might or will do in the future. Network operators want to
229 monetize this predictability and profit from it. On its
230 face, this is not an insidious practice. What is concerning
231 is that the market is largely unregulated.

232 In the digital age we can aggregate enormous amounts of
233 data, including what websites are viewed, search terms
234 entered, programs viewed, items bought and sold, web
235 applications utilized and other forms of data most of us
236 don't even realize is being collected. With this
237 information, a powerful profile can be created which can be
238 used to target specific advertisements that are more relevant
239 to the user.

240 We are here today to examine once again this growing
241 issue. How do we regulate personal data collected by web
242 companies and by network operators? Should we? And today we
243 are obviously focusing on the network operators.

244 There is a growing tide of critics in this debate that I
245 believe fundamentally do not understand the purpose of our
246 privacy laws. These voices, some of them testifying today,
247 believe that web-based services and telecommunications
248 carriers should be subject to the same privacy regulations.
249 I don't think this is practical or prudent. There is a
250 fundamental difference between offering up free web-based
251 advertiser supported applications and services, and a common
252 carrier offering voice and broadband services. These
253 separate and distinct services should each be governed
254 fairly. That doesn't mean within the same regulatory
255 structure. A healthcare provider and a stock broker

256 shouldn't be regulated, in my view, under the same structure.
257 Each should have its own. A consumer's relationship with
258 their phone or broadband provider is not the same
259 relationship they have with a search engine or an online
260 vendor.

261 I am eager to hear from all of our witnesses. I am glad
262 that you are all here today to hear about your practices and
263 how you would envision privacy regulations. This is a very
264 important debate and I hope that the final result will be a
265 very sound and prudent bill that can be taken to the floor of
266 the House.

267 So thank you, Mr. Chairman, for kicking off this series
268 of hearings.

269 [The prepared statement of Ms. Eshoo follows:]

270 ***** COMMITTEE INSERT *****

|
271 Mr. {Boucher.} Thank you very much, Ms. Eshoo.

272 The gentlelady from California, Ms. Bono Mack, is
273 recognized for 2 minutes.

274 Ms. {Bono Mack.} Good morning, Chairman Boucher,
275 Ranking Member Stearns and distinguished panel. Thank you
276 for holding a hearing on the important issue of consumer
277 privacy and broadband networks.

278 When a consumer makes a telephone call, purchases a good
279 online, visits a website or watches a TV program on his
280 couch, there is a built-in expectation of privacy associated
281 with each activity. It is understood that our personal
282 privacy is something of value. We have laws which protect
283 privacy and the assurance of privacy is a marketable quality.

284 It is also important to note that cost of certain
285 commercial activity on broadband networks is deflected away
286 from the consumer because of advertising. As many of you
287 know, I have a long history of working to protect consumers
288 in the online space. In past Congresses I authored anti-
289 spyware legislation and this is the second consecutive
290 Congress I have introduced the Informed P2P User Act,
291 therefore my legislative history speaks for itself.
292 Additionally, I also have a history of fighting to prevent
293 piracy online so I am willing to listen to efforts that

294 reduce the impact piracy has on our national economy, as
295 well.

296 As we begin the process of balancing consumer privacy
297 and commercial activities online, I would like to listen to
298 all sides of the debate and all parties involved in the
299 online space. This includes consumers, law enforcement,
300 ISPs, tech companies, search engines, advertisers, as well as
301 content creators. It is my belief that both the privacy
302 expectations and commercial activity need to be measured
303 before we act. The committee would be wise to begin with the
304 American consumers' privacy expectations in mind. I do not
305 look at this issue as a partisan matter and I don't think we
306 should be out to get one particular company or favor one
307 particular industry. With that said, I do admit that
308 sometimes a one size fits all approach is not possible in
309 achieving certain goals. As such, I will be paying close
310 attention to the debate and I look forward to working on this
311 important issue.

312 Thank you, Mr. Chairman. I yield back.

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

314 ***** COMMITTEE INSERT *****

|
315 Mr. {Boucher.} Thank you very much, Ms. Bono Mack.

316 The gentlelady from Colorado, Ms. DeGette, is recognized
317 for 2 minutes.

318 Ms. {DeGette.} Thank you very much, Mr. Chairman. I
319 want to thank you for having this important hearing today.

320 As technology changes and as consumer habits change, so
321 do the privacy concerns that we are faced with and so I am
322 looking forward to hearing from all of the witnesses today as
323 we continue in our evolving discussion of privacy.

324 And with that, I will yield back.

325 [The prepared statement of Ms. DeGette follows:]

326 ***** COMMITTEE INSERT *****

|
327 Mr. {Boucher.} Thank you very much, Ms. DeGette. We
328 will add 2 minutes to your time to question the panel of
329 witnesses based upon that waiver.

330 The gentleman from California, Mr. Radanovich, is
331 recognized for 2 minutes.

332 Mr. {Radanovich.} Thank you, Chairman Boucher. I want
333 to thank you and Mr. Stearns for holding this consumer
334 privacy meeting and I do want to thank you, Mr. Chairman, I
335 am pleased to hear that we will have a joint hearing on
336 online advertising. It will be important for us to hear from
337 the full technology landscape that utilizes private user
338 information before we can move forward with any comprehensive
339 effort to address this issue. I look forward to working with
340 you on that hearing, as well.

341 One of the primary issues that has developed with
342 communications and the Internet is the collection of consumer
343 data. As technology advances and becomes more complex,
344 consumers are rightfully concerned about their personal
345 information. What we should focus on when it comes to
346 consumer data is the consumers and what they care about and I
347 believe that we should invoke looking at what data is
348 collected, why it is collected and what is done with it.
349 This information will help us all work together with the

350 industry to achieve our goal of meeting the consumer needs by
351 preventing the misuse of their information.

352 What I think that we should be looking at for most is
353 the most effective way to protect our constituents'
354 information in a manner that recognizes there are beneficial
355 users for many of these new technologies and continues to
356 allow for innovation that can make the communications
357 experience more enjoyable, more productive and safer for us
358 all.

359 I want to thank all of our witnesses for being here
360 today and to discuss a wide variety of networks and their
361 relationship to privacy. Your experience will certainly help
362 us as we continue and I look forward to a productive hearing.

363 Thank you, Mr. Chairman.

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

365 ***** COMMITTEE INSERT *****

|
366 Mr. {Boucher.} Thank you, Mr. Radanovich.

367 The gentleman from Michigan, Mr. Stupak, is recognized
368 for 2 minutes.

369 Mr. {Stupak.} Thank you, Mr. Chairman, and thank you
370 for holding this hearing.

371 It is time we modernized our telecommunications policies
372 in regard to privacy. An individual's right to privacy has
373 been under increasing assault as more Americans are using the
374 Internet for more and more of their daily activities.
375 Consumers do not have a clear picture of what occurs with
376 their information without their consent and what needs to be
377 done.

378 Last year this subcommittee held a hearing on a new type
379 of data gathering for the purpose of behavioral advertising.
380 This new method uses network technology known as deep pack
381 inspection to read 100 percent of a web user's activities to
382 create a profile for purposes of reselling it to advertisers.
383 Companies that wish to utilize this technology have claimed
384 that personally identifiable information is protected but I
385 have my doubts and concerns.

386 As it stands right now, The Communication Act gives no
387 clear definition of when affirmative consent or opt-in is
388 required in the handling of a consumer's personal

389 identifiable information. Without clear direction from
390 Congress on this matter, technology will continue to outpace
391 our privacy laws and consumer personal information will
392 continue to go unprotected. Any method of collecting
393 personally identifiable information from an Internet user's
394 online activity for the purpose of reselling that information
395 must require an opt-in from that user. In addition, that
396 user should also be provided with the information on how and
397 what is happening with their data, how it is collected and
398 who is receiving it.

399 I look forward to hearing from our witnesses today on
400 how we can modernize our privacy laws to protect, inform and
401 empower consumers.

402 Thank you, Mr. Chairman, again for holding this hearing.
403 I look forward to working with you and our colleagues to move
404 legislation on this subject.

405 [The prepared statement of Mr. Stupak follows:]

406 ***** COMMITTEE INSERT *****

|
407 Mr. {Boucher.} Thank you very much, Mr. Stupak.

408 The gentlelady from Tennessee, Ms. Blackburn, is
409 recognized for 2 minutes.

410 Ms. {Blackburn.} Thank you, Mr. Chairman. I want to
411 thank you for holding the hearing today. And I want to
412 welcome all of our witnesses and thank you for being here
413 with us today.

414 Consumer privacy as you have heard from everyone who has
415 spoken is a key element in the unspoken contract between the
416 end user and the ISP and the merchants who make their living
417 providing goods and services online. When any link in that
418 chain of trust is broken, consumers at every level are going
419 to suffer. It is therefore critical for Congress and our
420 partners in the administration, the private sector and the
421 consumer advocacy community to remain vigilant in securing
422 consumer privacy online.

423 It is also critical on the other hand that Congress
424 ensure vibrancy in the marketplace. And I think that is
425 where many of us are going to have questions and want to
426 explore a little bit more deeply with you to make certain
427 that we have a good understanding of the deep packet
428 inspection technologies and that we move forward in the
429 appropriate way.

430 Mr. Chairman, I am pleased to know that we are going to
431 do another hearing on the Google issues that are in front of
432 us and I look forward to working with you on that hearing.
433 And I hope that we can all send a message that piracy does
434 not pay. That privacy and respect for intellectual property
435 is an imperative and I look forward to the hearing.

436 I yield back.

437 [The prepared statement of Ms. Blackburn follows:]

438 ***** COMMITTEE INSERT *****

|
439 Mr. {Boucher.} Thank you very much, Ms. Blackburn.

440 The gentlelady from Florida, Ms. Castor, is recognized
441 for 2 minutes.

442 Ms. {Castor.} Thank you, Mr. Chairman, for this timely
443 hearing on the evolution of our communications networks and
444 consumer privacy. Welcome to our panel. I look forward to
445 your expert advice in learning a great deal more about this
446 issue and I will yield back the remaining portion of my time.

447 [The prepared statement of Ms. Castor follows:]

448 ***** COMMITTEE INSERT *****

|
449 Mr. {Boucher.} Thank you very much, Ms. Castor. We
450 will add 2 minutes to your questioning time for the first
451 panel.

452 The gentleman from Nebraska, Mr. Terry, is recognized
453 for 2 minutes.

454 Mr. {Terry.} Thank you, Mr. Chairman. I would waive
455 and appreciate 2 minutes.

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

457 ***** COMMITTEE INSERT *****

|

458 [The prepared statement of Mr. Markey follows:]

459 ***** INSERT 8 *****

|

460 Mr. {Boucher.} You shall have the same. All members
461 having now been recognized for opening statements, we turn to
462 our panel of witnesses and express appreciation to each of
463 you for your testimony here this morning. Ms. Leslie Harris
464 is the president and chief executive officer of the Center
465 for Democracy and Technology. Mr. Kyle McSlarrow is
466 president and chief executive officer of the National Cable
467 and Telecommunications Association. Mr. Marc Rotenberg is
468 the executive director of the Electronic Privacy Information
469 Center. Ms. Dorothy Attwood is chief privacy officer for
470 AT&T Services. Mr. Ben Scott is policy director for Free
471 Press. Mr. Brian Knapp is chief operating officer of Loopt.
472 And Mr. Richard Bennett is a network engineer and a blogger
473 and we welcome each of you. Without objection, your prepared
474 written statements will be made part of the record. We would
475 ask for your oral summary kept to approximately 5 minutes so
476 that we will have ample time for questions.

477 And, Ms. Harris, we are pleased to begin with you and
478 you need to turn your mike on. It is amazing how many people
479 in the technology subcommittee don't have their mike on when
480 they start to testify.

|

481 ^STATEMENTS OF LESLIE HARRIS, PRESIDENT, CHIEF EXECUTIVE
482 OFFICER, CENTER FOR DEMOCRACY AND TECHNOLOGY; KYLE MCCLARROW,
483 PRESIDENT AND CEO, NATIONAL CABLE AND TELECOMMUNICATIONS
484 ASSOCIATION; MARC ROTENBERG, PRESIDENT AND EXECUTIVE
485 DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER; DOROTHY
486 ATTWOOD, SENIOR VICE PRESIDENT, PUBLIC POLICY AND CHIEF
487 PRIVACY OFFICER, AT&T SERVICES, INC.; BEN SCOTT, POLICY
488 DIRECTOR, FREE PRESS; BRIAN R. KNAPP, CHIEF OPERATING
489 OFFICER, LOOPT, INC.; AND RICHARD BENNETT, PUBLISHER,
490 BROADBANDPOLITICS.COM

|

491 ^STATEMENT OF LESLIE HARRIS

492 } Ms. {Harris.} Mr. Chairman, Mr. Stearns, members of the
493 subcommittee, I appreciate the opportunity to testify on this
494 important question of the privacy implications of DPI.

495 In CDT's view, DPI poses very serious challenges both to
496 the privacy and to the openness of the Internet. The success
497 of the Internet can be traced to its defining end-to-end
498 principle which is a simple idea that applications are better
499 left to be implemented at the edges of a network and leave
500 the core unfettered by gatekeepers.

501 The end-to-end principle, as you know, is supported by a

502 policy framework that generally protects Internet service
503 providers for liability for the content that they are either
504 posting or flowing over their networks. And together these
505 two policy choices have really preserved the Internet as a
506 trusted, open platform.

507 Today massive growth in data processing power has
508 spurred the development of DPI and potentially allowing
509 Internet service providers and other intermediaries and
510 partners to analyze all of the Internet traffic of millions
511 of users simultaneously. This raises profound questions
512 about the future of privacy, openness and innovation online.
513 Though deployment is still somewhat limited, applications
514 range from management of congestion on the networks and
515 network threats, content blocking, behavioral advertising and
516 government surveillance.

517 It is my understanding that right now network operators
518 are only using the technology for security-related purposes
519 although, of course, last summer we did have a failed attempt
520 to use it for behavioral advertising. Of course, some of
521 these applications may have other troubling legal policy
522 concerns but it is important to stress that all applications
523 of DPI raise serious privacy concerns because all
524 applications of DPI begin with the interception and analysis
525 of traffic.

526 In our view, deep packet inspection is really no
527 different than postal employees opening envelopes, reading
528 letters inside. DPI networks intercept and examine the
529 entire payload of a packet, the actual data that the packet
530 carries in addition to a packet header unless the content is
531 encrypted.

532 So even if ISP's or advertising networks intend to only
533 use a small portion of what is captured by DPI and dispose of
534 the rest, it doesn't diminish the breadth and intrusiveness
535 of that initial data capture. And DPI is being deployed
536 within a technological environment where consumers are
537 sending more and more information through the networks.
538 Providers of all kinds are acquiring and collecting and
539 holding more data and sharing it and it is being retained for
540 longer periods of time and all of this without an adequate
541 legal framework.

542 Consumers simply do not expect to be snooped on by their
543 ISPs or other intermediaries in the middle of the network.
544 And so therefore DPI really defies the legitimate
545 expectations of privacy that consumers have and it is also at
546 odds with fair information practices, concepts like
547 transparency, concepts like limited collection of data. The
548 sectoral privacy laws that we have, have been far outpaced by
549 technological innovation and as many of you have said, we

550 have no baseline consumer privacy law.

551 Finally, as DPI matures and becomes more widely
552 deployed, our concern is that any notion of limited use is
553 going to give way to mission creep as new applications are
554 deployed. And that mission creep, frankly, is not just a
555 concern that the providers will find new ways but that
556 government and policymakers will increasingly have mandates
557 to networks to use DPI for various purposes. And, of course,
558 we worry as well about the sort of unlimited appetite for
559 surveillance that our government appears to have and the fact
560 that DPI really is a game changer there as well.

561 For all these reasons, we applaud the fact you are
562 taking a comprehensive look at DPI. We obviously think that,
563 you know, the most important thing that can happen this year
564 is an acting baseline, technology neutral consumer privacy
565 legislation based on fair information practices. We are very
566 pleased to hear the announcement, Mr. Chairman, and the
567 support from the committee. I will just say that we also
568 hope the subcommittee might move ahead with carefully crafted
569 Internet neutrality legislation because we think it might put
570 some balance on the more worrisome uses of DPI. And finally,
571 it is outside of your jurisdiction, I think, but Congress has
572 to examine and strengthen the communications privacy laws,
573 ECPA, et cetera, at the same time which has to do with

574 government access because all of these have been outstripped
575 by technology and really change the nature of what privacy
576 protections really exist at this point for consumers.

577 So thank you so much.

578 [The prepared statement of Ms. Harris follows:]

579 ***** INSERT 1 *****

|
580 Mr. {Boucher.} Thank you very much, Ms. Harris.

581 Mr. McSlarrow.

|
582 ^STATEMENT OF KYLE MCCLARROW

583 } Mr. {McClarrow.} Mr. Chairman, Mr. Stearns,
584 distinguished members of the subcommittee, thank you for
585 giving me an opportunity to testify today.

586 I think the starting place for the cable industry is to
587 recognize that Congress passed probably what was at that time
588 the first broad based opt-in statute, a very forward-leaning,
589 pro-consumer, privacy protection regime that we have lived
590 under for over 25 years for cable services. And today with
591 digital voice services, we now live under the similar privacy
592 protections offered under Section 222 of The Communications
593 Act. And during that time I think our track record has been
594 excellent both in terms of safeguarding consumer privacy and
595 abiding by rules that I think people have discovered prove
596 that good privacy protection is also good business so we
597 believe that.

598 As I think everybody has acknowledged, the question on
599 the table isn't so much what people are doing today. It is
600 about the emerging models and emerging ideas in creativity
601 and what they mean for privacy, and we think it is completely
602 appropriate to examine all of that.

603 In the short time I have available, I do want to take a

604 deeper dive into deep packet inspection because I think it is
605 actually emblematic of this entire conversation. It is true
606 that today, at least for my members, none of the cable ISPs
607 are actually using any of this information for behavioral
608 targeting purposes. But obviously, there are many industries
609 including ours who are interested in trying to figure out a
610 way to provide more relevant and useful advertising for the
611 consumer. It is likely to support the entire Internet
612 ecosystem. It is likely to spur more growth in creative
613 ideas and content and services, but we recognize that it has
614 to be done in a way that is respectful of the consumer's
615 privacy.

616 Deep packet inspection is actually not something that is
617 new. One of the frustrations I think we have is that people
618 act like something just happened yesterday, something new and
619 different and scary. Deep packet inspection or packet
620 inspection generally is something the operators, all
621 providers have used or tools like that for many years and for
622 very good reasons. I think the test is consumer expectations
623 and I think broadly speaking, when a consumer sits down at a
624 computer it is always on if they are a broadband customer.
625 They go anywhere they want. They access any application they
626 want. No one stops them. It all works. The speeds are
627 doubling. The price per megabyte is dropping. Deployment is

628 continuing but on the other side of that computer, there is a
629 war going on. You have got network operators who are
630 fighting malware and viruses and spam. You have got botnet
631 armies and things that I don't even know about that are
632 taking place in very complicated regime. The consumer
633 doesn't know anything about that. They don't want to know
634 anything about that. They don't necessarily need to know how
635 you are dealing with it. They just want you to deal with it
636 and we do.

637 Now, I think reading everybody's testimony, I think
638 everybody concedes that the use of deep packet inspection has
639 today beneficent and pro-consumer purposes so I am not going
640 to dwell on that. But I will say there it is hard to do
641 analogies because probably no one in this room or very few
642 are really technical experts here. But I do think we have to
643 be very careful. We require some precision here when we are
644 talking about deep packet inspection.

645 I have heard and I think Leslie just said as an example,
646 this is like the post office opening up your letter, going
647 beyond looking at the address and looking at the contents of
648 the letter. And I myself am guilty sometimes just saying a
649 packet of information on the Internet has a header and a
650 payload. But the truth is if you are looking at the layers
651 of a packet, each layer has a header and payload. Each, you

652 know, one layer, layer four is going to be something, you
653 know, that has source and destination for IP addresses, all
654 the way down to layer seven where you could have a web
655 browser, URL address, source and destination. And when you
656 hear envelope and content you think there is just one step
657 before you get to the content but the truth is, it is really
658 more like envelopes within envelopes, each one of which has
659 addresses and at some point you do have content.

660 So far as I can tell, I haven't done my own due
661 diligence, the only time we are actually scanning and what I
662 mean by scan, I mean a machine doing something in a billionth
663 of a second, content is what we are trying to deter spam.
664 All of the other activities related to deep packet
665 inspections so far as I am aware, are looking at headers.
666 That is the addresses that most people say they are actually
667 okay with.

668 So my point here is just a caution. Any technology can
669 be used for good purposes and for bad. We recognize that no
670 one would want us looking at the communications in an e-mail.
671 We don't particularly want to do that. In fact, the only
672 tracking I actually want to do is to track down the engineer
673 who actually came up with the term deep packet inspection and
674 shoot him.

675 Last point and I realize I am rowing against the tide

676 here and you do have my commitment, Mr. Chairman, that as you
677 consider legislation to work constructively with you but I do
678 want to make a final plea to consider allowing self-
679 regulation to work and I would really say it for two reasons.
680 Number one, this entire arena is moving so fast. There are
681 new models being created. I know that is what gives rise to
682 the concerns but I also think it is a caution. It is very
683 hard to freeze one point in time with what is actually a
684 fairly immature marketplace when you think about it how young
685 the Internet system is and how young really the broadband
686 market is. And I think we should allow industry and all
687 stake-holders to try to work together using the oversight of
688 this committee and the bully pulpit, force us to come up with
689 self-regulatory principles that respect consumers' privacies
690 knowing that at least in my industry's case, we have a
691 backstop of legislation that gives a lot of the rules of the
692 road. And the second is to recognize that behavioral
693 advertising can potentially be the most pro-consumer thing we
694 do to enrich the Internet to allow new services that haven't
695 even been created yet to survive and thrive by making it easy
696 for those services new web applications to monetize their
697 services without having to go out and get the capital
698 necessary to launch a new service.

699 Thank you, Mr. Chairman.

700 [The prepared statement of Mr. McSlarrow follows:]

701 ***** INSERT 2 *****

|

702 Mr. {Boucher.} Thank you, Mr. McSlarrow.

703 Mr. Rotenberg.

|
704 ^STATEMENT OF MARC ROTENBERG

705 } Mr. {Rotenberg.} Thank you, Mr. Chairman and members of
706 the committee. I appreciate the opportunity to be here
707 today.

708 EPIC has a broad interest in matters of consumer privacy
709 and network security. We have worked on technical issues at
710 ICANN and IETF on the evolving standards for Internet
711 security. We have been at the FCC on rule-making for
712 consumer privacy and we have even defended the commission's
713 authority to enforce consumer protections on the network. So
714 we have a broad understanding I think of the issues and the
715 opportunities to safeguard consumers in this emerging online
716 environment and I agree very strongly with the members of the
717 committee who say that this is a vital issue for consumers
718 today. According to the Federal Trade Commission, identity
719 theft is the number one concern of American consumers. We
720 have serious problems also with security breaches and so the
721 need to find a policy here that makes it possible to take
722 advantage of new technology to grow new business
723 opportunities and at the same time to safeguard consumers is
724 absolutely critical.

725 Now, let me say a few words about the DPI issue and I

726 should add I have also been teaching privacy law for many
727 years over at Georgetown. One of the things that has
728 occurred to me is that many of these issues that may seem new
729 today, in fact have been with us for a very long time. So I
730 want to say a few words now about The Communications Act of
731 1934. The Communications Act of 1934 set out the first
732 regulatory framework for communication service providers in
733 the United States and it tried to answer a simple question,
734 in part. Under what circumstances should communication
735 service providers get content to the information that they
736 are conveying on behalf of their customers. And the answer,
737 generally speaking, was to ensure the provision of the
738 service to make sure that it worked and to protect security
739 and to comply with a legal requirement provided by the
740 government such as a warrant. And there really were no other
741 exceptions which is to say you could listen in on the
742 telephone to make sure your line was working, and you could
743 deal with load leveling issues, and you could enforce a
744 wiretap if you were told to do so but you weren't supposed to
745 access the communications traffic for your own commercial
746 benefit.

747 And I think that commonsense understanding of the
748 obligations of communication service providers answers most
749 of the questions that have been asked about deep packet

750 inspection today. I do not think that companies that are in
751 the business of providing network services to customers
752 should get access to the content of the communications for a
753 commercial benefit. There may be other good reasons, spam,
754 viruses, legal obligations which I think we would all accept
755 are appropriate exceptions but broadly speaking I don't think
756 there should be access.

757 Now, here is where it gets interesting. The companies
758 that have come along in the last couple of years such as
759 NebuAd and Phorm have said we have a way to get access to the
760 traffic that doesn't require us to know who the individual
761 users are. We are going to do this type of targeting without
762 collecting personally identifiable information which from a
763 privacy perspective is actually very attractive because our
764 big concern, of course, is that if companies know who these
765 users are they build very detailed profiles and people just
766 won't know how much information about them is being
767 collected. And so NebuAd and Phorm, both companies that have
768 been highly criticized for their technique are at the same
769 time developing some of the most innovative methods for
770 advertising because they are genuinely concerned about
771 privacy.

772 Now, this actually creates for you a very interesting
773 dilemma. I don't think it solves the intercept problem

774 because the truth is they are still going to the network
775 without affirmative consent and they are still getting access
776 and I think they are still violating The Wiretap Act as many
777 of the members of this committee concluded last year and as
778 European Commission Vivian Redding said early this month when
779 she brought an action against the Government of Great
780 Britain for allowing the service to go forward. So the
781 intercept problem is still there but the question is let us
782 say people agreed. Let us say people said well if you can do
783 this advertising well and you are not profiling me maybe I am
784 okay with that and I think you still have a policy challenge.
785 I think you have to ensure that these new services really do
786 protect the anonymity of the users, really ensure that it
787 doesn't become possible later to figure out who these folks
788 are or don't simply decide to change the business model.

789 Now, why should you be concerned about that and why do
790 you ultimately need to legislate because that is actually
791 what happened 10 years ago with online advertising. When a
792 company called DoubleClick said we can make anonymous
793 advertising work on the Internet, many of us supported that.
794 Many companies partnered with DoubleClick and then
795 DoubleClick said well now that we got all of these people in
796 our advertising base, maybe we should start identifying them.
797 And that actually began the first wave of hearings on the

798 issue of Internet privacy when people were being targeted
799 because of who they were without adequate privacy protection.
800 And I think that will be a critical question in this specific
801 context for this committee to address.

802 Mr. Chairman, if I would make one final point and I very
803 much appreciate the fact that you have held this hearing and
804 plan to hold another hearing, I do think from the user
805 perspective we can't limit the discussion to concerns about
806 DPI. There are a lot of other activities that implicate
807 online privacy, web-based e-mail for example. I mean I am
808 surprised that companies are able to get access to the
809 content of e-mail and provide advertising on that basis.
810 From the user's perspective that is the functional equivalent
811 of the carrier getting access to the message and providing
812 some, you know, commercial benefit. It is a difficult
813 question that hasn't been addressed yet but I hope the
814 committee will get to that one, as well.

815 Thank you very much.

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

817 ***** INSERT 3 *****

|

818 Mr. {Boucher.} Thank you, Mr. Rotenberg.

819 Ms. Attwood.

|
820 ^STATEMENT OF DOROTHY ATTWOOD

821 } Ms. {Attwood.} Thank you, Chairman Boucher and Ranking
822 Member Stearns for providing AT&T the opportunity to discuss
823 consumer privacy in the online world.

824 As the leading communications company in America, AT&T
825 has a profound interest as a major advertiser, as a website
826 publisher, as an Internet service provider and as a provider
827 of communications generally, in seeing the Internet grow
828 through an advertising-supported model. After all, online
829 advertising fuels investment and innovation across a wide
830 range of Internet activities and next generation forums of
831 online advertising could prove quite valuable to consumers
832 and could dramatically improve their online experiences.

833 At the same time, we balance our interest in the
834 evolution of online advertising with the unique investment we
835 have in concentration on our customer relationships. These
836 relationships are our most treasured asset and we are
837 doggedly focused on enhancing them and ensuring that our
838 customer expectations are met. For this reason, AT&T has
839 articulated and publicly supports a pro-consumer framework
840 that both promotes the privacy interests of our customers as
841 well as fostering advancements that lead to more useful and

842 relevant online advertising. We have endorsed the simple
843 principle that we need to engage consumers and offer them
844 transparency and control over their Internet experience.

845 The new forms of online advertising that is the subject
846 of today's hearing which we generally refer to as behavioral
847 advertising, can take many forms. They can in theory involve
848 the use by an ISP of technologies such as deep packet
849 inspection to capture and analyze a user's Internet browsing
850 activities and experience across unrelated websites. They
851 also involve search engines and advertising networks
852 implementing evermore sophisticated technologies to track
853 consumer web surfing and search activity over time, to
854 develop profiles of consumer activity and combine data from
855 offline and online sources. They are not inherently
856 problematic but pitfalls can arise because behavioral
857 advertising in its current forms is largely invisible to
858 customers.

859 We have actually conducted focus groups and we have
860 asked our customers their views on behavioral advertising and
861 the results have been illuminating. Customers clearly appear
862 to understand and willingly accept that information will be
863 collected in commercial relationships and will be used to
864 offer goods and services that are of value to them. But
865 these same consumers do not well understand and fully embrace

866 the concept that their online activity associated across
867 unrelated websites or their overall web browsing activity can
868 be and is used today to create detailed profiles of them.
869 They can see the benefits of more targeted and relevant
870 advertising but they want control over their personal
871 information and they want that control to be individualized.

872 These new online advertising paradigms must therefore be
873 designed to account for a new set of still evolving customer
874 expectations about how personal information will be used and
875 how personal privacy will be safeguarded. As an industry
876 then, we must deploy next generation advertising techniques
877 in tandem with next generation privacy innovations and any
878 solution must be achieved by all elements of the Internet
879 ecosystem.

880 For its part, AT&T is listening to its customers and we
881 are confronting the opportunities and challenges presented by
882 behavioral advertising by not thoughtlessly lurching into
883 this realm. We will initiate such a program only after
884 testing and validating the various technologies and only
885 after establishing clear and consistent methods and
886 procedures to engage customers, to ensure the protection of
887 and ultimately their control over their information. If AT&T
888 deploys these technologies and processes, we will do it the
889 right way. So indeed, AT&T has already adopted flexible

890 privacy principles that will guide any effort to engage in
891 behavioral advertising, the pillars of which are
892 transparency, customer control, privacy protection and
893 customer value. These principles can be the foundation of an
894 ethic of consumer engagement for all players in the online
895 behavioral advertising sphere and it both ensures that
896 customers have ultimate control over the use of their
897 personal information and guards against privacy abuse.

898 I want to thank you very much and look forward to your
899 questions.

900 [The prepared statement of Ms. Attwood follows:]

901 ***** INSERT 4 *****

|

902 Mr. {Boucher.} Thank you very much, Ms. Attwood.

903 Mr. Scott.

|
904 ^STATEMENT OF BEN SCOTT

905 } Mr. {Scott.} Thank you, Chairman Boucher and Ranking
906 Member Stearns and members of the subcommittee.

907 I am the policy director for Free Press. We are the
908 largest public interest organization in the country that
909 works on media policy issues. I would like to focus my
910 testimony this morning on deep packet inspection or DPI. I
911 have submitted a white paper on the subject for the record
912 which I will try to summarize here.

913 You have already heard about the uses for DPI for the
914 collection of personal information about Internet users for
915 advertising purposes. I would like to focus on other issues
916 of DPI technology because really any time a network monitors
917 Internet traffic as Mr. Rotenberg pointed out, we have a
918 potential privacy problem. That harm is compounded by DPI
919 tools that violate network neutrality with any competitive
920 practices.

921 Let me offer a little context. It is 3 years ago we had
922 a robust debate in the Congress over the necessity of net
923 neutrality and privacy rules to protect the consumers, and
924 that debate largely turned on whether or not the harms were
925 hypothetical, and indeed the technology did not exist in 2006

926 that would have permitted wide-scale violations. Today these
927 technologies do exist. They are deep packet inspection
928 devices and they are now widely deployed. Worse still, from
929 my perspective, an entire industry of manufacturers has
930 emerged that markets DPI explicitly to monitor and control
931 consumer behavior online. All a network operator has to do
932 is flip the switch.

933 DPI will have a broad impact on the Internet. Without
934 this technology, everything you do online is sent through the
935 network basically anonymously, e-mail, sports scores, family
936 photos. The network doesn't know or care what you are doing.
937 Online anonymity in this sense also has the virtue of
938 nondiscrimination. But with DPI, it is a whole new ballgame.
939 This technology can track every online click. Once a network
940 owner can see what you are doing, they have the power to
941 manipulate your experience. They can sell you ads. They can
942 block content. They can speed things up. They can slow
943 things down. Perhaps there is no better way to describe what
944 DPI can do then to quote directly from the manufacturers'
945 marketing materials. Their selling points are exactly the
946 uses that trouble me most.

947 Let me offer a few examples. Zeugma Systems describes
948 its technology as a way for network owners to ``see, manage
949 and monetize individual flows to individual subscribers.'' A

950 company called Allot promises that their equipment empowers
951 ISPs ``to meter and control individual use of applications
952 and services'' including to help network owners ``reduce the
953 performance of applications with negative influence on
954 revenues (e.g. competitive VoIP services).'' Now, that
955 sounds like blatantly anti-competitive behavior to me.
956 Procera Networks went so far as to publish a brochure that
957 was titled ``If You Can See It, You Can Monetize It.'' That
958 is chilling stuff and there are more than a dozen of these
959 companies. I could go on and on. They sell products
960 marketed to help ISPs make more money by spying on consumers
961 and controlling how they use the Internet.

962 Let me be clear, the technology itself is not
963 necessarily problematic. However, in the past year deep
964 packet inspection has evolved from basically innocuous to
965 potentially insidious. DPI was created as a network security
966 tool but has become a mechanism of precise surveillance and
967 content control. We have already begun to see incidents of
968 bad behavior.

969 This subcommittee has had hearings on Comcast and NebuAd
970 which both used DPI in secret, questionable ways. Today, Cox
971 Communications is using DPI to speed up some applications and
972 slow down others. These types of practices may have short
973 term traffic management benefits but the tradeoff is the

974 unprecedented step of putting a network owner in control of
975 consumers' online choices. After this first step, it is a
976 slippery slope. We could soon see every major ISP in the
977 country adopt a different traffic control regime. Without
978 oversight, this could vulcanize the Internet so that
979 applications that work on a network in Virginia may not work
980 on a network in Kansas or Florida.

981 The critical question is how to best protect consumers
982 from these kinds of harms. Let me offer an analogy. Think
983 of DPI technologies as similar to complex financial
984 instruments like, I don't know, credit default swaps.
985 Properly regulated they can be used as a constructive part of
986 our banking system. But without oversight, they can run
987 amuck and severely harm consumers.

988 What we need are bright line rules of consumer
989 protections. The negative implications for privacy network
990 neutrality are already clear but the new uses of DPI may also
991 reduce incentives for infrastructure investment. Installing
992 DPI offers a tempting alternative to building a robust
993 network. At a fraction of the cost, a DPI can discourage
994 users from high-bandwidth applications or charge higher fees
995 for priority access.

996 Before these technologies become firmly entrenched, we
997 encourage Congress to open a broad inquiry to determine what

998 is in the best interest of consumers. Once DPI devices are
999 activated across the Internet, it will be very difficult to
1000 reverse course.

1001 I thank you for your time and I do look forward to your
1002 questions.

1003 [The prepared statement of Mr. Scott follows:]

1004 ***** INSERT 5 *****

|

1005 Mr. {Boucher.} Thank you, Mr. Scott.

1006 Mr. Knapp.

|
1007 ^STATEMENT OF BRIAN R. KNAPP

1008 } Mr. {Knapp.} Good morning, Chairman Boucher, nice to
1009 see you again, Ranking Member Stearns and members of the
1010 subcommittee.

1011 My name is Brian Knapp, Chief Operating Officer. I have
1012 responsibility at Loopt for day-to-day business operations as
1013 well as privacy policy, data security matters and legal
1014 affairs.

1015 Since you may not be familiar with my company, Loopt,
1016 please allow me to tell you a little bit about our company.
1017 We are a location-based service that can change the way
1018 friends and family connect, share and explore in the mobile
1019 environment. Loopt facilitates real world interactions by
1020 helping users connect on the go and navigate their social and
1021 family lives. Loopt users can see their friends and family
1022 where they are located and what is going on around them via
1023 detailed interactive maps on their mobile phones. And users
1024 can also share location information and updates with their
1025 networks of friends on a variety of popular social networks
1026 and communities. Over one million users have already
1027 registered for Loopt and by all accounts, consumers are very
1028 excited about emerging mobile services and location services

1029 like Loopt.

1030 Loopt itself got started back in 2005 when Sam Altman, a
1031 sophomore computer science major at Stanford University had
1032 an epiphany as he walked out of class, realizing that it
1033 would be great if he could open his mobile phone and see a
1034 map of where all his friends were. Since 2005, Loopt has
1035 grown. We are located in Mountain View, proud to be in
1036 Congresswoman Eshoo's district. We have grown to over 40
1037 employees and our service is launched across multiple
1038 wireless carriers and mobile devices.

1039 Today we are available on AT&T Mobility, Sprint Nextel,
1040 Boost Mobile, MetroPCS, T-Mobile and Verizon Wireless
1041 networks as well as popular devices such as the Apple iPhone,
1042 Blackberry and Google's Android G1. Depending on the service
1043 provider and the device, the cost of Loopt ranges from free
1044 and advertising-supported to \$3.99 per month.

1045 From its inception, Loopt's founders and investors made
1046 a commitment to the development of strong privacy practices
1047 and policies. I began working with the company in late-2005
1048 and was hired full-time by the company as chief privacy
1049 officer and general counsel two years ago, and they asked me
1050 specifically to focus on these areas as we developed our
1051 service and grew the company. At that time, we only had 13
1052 other employees and we were alive on one network operator at

1053 the time. However, even in our early days we knew that
1054 investing in an effective privacy program was necessary for
1055 our users and an important foundation for our future business
1056 growth and success.

1057 Our privacy approach is based on the key principles of
1058 user-control, education and notice and our regime
1059 specifically includes informed consent. Our service is 100
1060 percent permission-based so users are choosing to download
1061 and access Loopt. We receive this informed consent from
1062 every user. They must proceed through a multi-step
1063 registration process which has key information about how the
1064 service works and how they should use it responsibly. And
1065 there are several ways to access our key user agreements and
1066 privacy policies. At the end of my testimony there is
1067 actually a flow of this process that you can see.

1068 We have reminders and notifications even after users
1069 have registered to again have them keep in mind how to use
1070 the service responsibly and access the privacy settings.
1071 Speaking of privacy settings, we have several controls so
1072 they can manage where, when and with whom their location is
1073 shared and displayed.

1074 Also, any friend connections or family connections made
1075 on Loopt are also chosen by the user so there is no automatic
1076 sharing of location information. You have to decide who you

1077 are going to share that information with and then you can
1078 still control it after the fact.

1079 We also have age limits on our service so our minimum
1080 age is 14 years and we have implemented an age-neutral
1081 screening mechanism in compliance that works in accordance
1082 with the FTC's guidance with regard to COPPA best practices.
1083 We have report abuse links throughout the service so the
1084 community can give us feedback if other users seem to be
1085 behaving badly. Our privacy notice and user education are
1086 key aspects of our regime. Our privacy notice is readily
1087 available and viewable within the mobile application itself
1088 and on our website and may actually be received by e-mail or
1089 postal delivery for our users. Our website contains detailed
1090 information about our privacy features as well as frequently
1091 asked questions and there are several links on the homepage
1092 of that site to access this information.

1093 I want to emphasize that we have developed these
1094 policies by listening to our customers and working closely
1095 with leading mobile social networking and online privacy and
1096 security organizations, including the Center for Democracy
1097 and Technology, the Electronic Frontier Foundation, the
1098 Family Online Safety Institute and Progress and Freedom
1099 Foundation, among others.

1100 We also participated in an Internet safety technical

1101 task force and finally, we also participated in the
1102 development of CTIA's Guidelines and Best Practices for
1103 Location-Based Services. And our accomplishments to date in
1104 terms of privacy and security innovation would not have been
1105 possible without the great feedback, insights and know-how of
1106 these organizations and folks on the hill.

1107 We believe that the result of all this collaboration is
1108 a consistent, sound set of privacy policies that apply to all
1109 of our users, regardless of where they live or use the
1110 service. We know that Loopt's customers value their privacy
1111 and especially the easy access to tools and information to
1112 control their privacy settings as needed so we have created a
1113 privacy policy and regime that is both straightforward,
1114 effective and easy to understand. We do note that this is an
1115 evolutionary process.

1116 We look forward to participating in these hearing and
1117 learning from other companies and the hill. And we will
1118 continue to strive for excellence in privacy innovation and
1119 aspire as a company to achieve effective privacy by design.

1120 Thank you for the opportunity to share our story and I
1121 look forward to any questions you may have.

1122 [The prepared statement of Mr. Knapp follows:]

1123 ***** INSERT 6 *****

- |
- 1124 Mr. {Boucher.} Thank you, Mr. Knapp.
- 1125 Mr. Bennett.

|
1126 ^STATEMENT OF RICHARD BENNETT

1127 } Mr. {Bennett.} Good morning, Mr. Chairman, Mr. Stearns
1128 and members.

1129 Thanks very much for inviting me. This is the first
1130 Congressional meeting I have actually attended in person
1131 since Senate Watergate. So maybe I should tell you what I
1132 know and when I came to know it.

1133 I am actually--some said there are no technical experts
1134 here. I am kind of offended by that because I am supposed to
1135 be one. I have been developing network systems for some 30
1136 years in the Ethernet and Wi-Fi systems that use today
1137 include some innovations that I personally invented and put
1138 there. And so when I look at these technologies the sort of
1139 collection of technologies that are coming under the umbrella
1140 of deep packet inspection, I think I have a slightly
1141 different perspective on it than most people do because what
1142 I see them as is an evolution of the tools that we have used
1143 to develop network technologies over the years.

1144 It has been essential in the development of every
1145 network protocol and in every network access device to have
1146 intelligence about the behavior of the systems that are
1147 communicating and the forwarding behavior of the intermediate

1148 nodes and the network that move the packets along. Without
1149 the ability to have that information we would not have been
1150 able to develop the systems that we all use today on the
1151 Internet and on the related private networks that feed the
1152 Internet.

1153 We never called this deep packet inspection. We simply
1154 called it packet monitoring and that process which was
1155 largely a matter of running a system that had filters that
1156 could capture packets from a live network and store them for
1157 the immediate examination and analysis by a network engineer,
1158 has been automated into a system that takes that information
1159 that has always been accessible to network engineers. There
1160 is not any--I mean I take issue with Mr. Scott that there has
1161 been some new leap forward in this technology in the last
1162 year. I mean there really hasn't. It is a smooth evolution
1163 from the systems that we have always used for manual analysis
1164 into archiving and data-mining, and these are the features
1165 that have actually changed in the use of this technology over
1166 the years.

1167 The raw information has always been there and the raw
1168 information is there because digital networks typically don't
1169 carry encrypted traffic. And the reason for that is a lot of
1170 the information that you might think of as payload is
1171 actually header from another point of view as Mr. McSarrow

1172 indicated. When we examine a network packet there is in fact
1173 a series of headers that you get that you have to go through
1174 before you get to final payload. And there is no actual
1175 location in that packet where you can draw a bright line and
1176 say everything to the right of this is payload, everything to
1177 the rest is header because applications invent protocols on
1178 top of protocols, on top of protocols and it is a more or
1179 less never-ending process because that is how new services
1180 are born on the web.

1181 So I am not worried about the use of deep packet
1182 inspection if I can use that term for network management
1183 purposes. For network management purposes it is vitally
1184 important for network operators to be able to apply network
1185 engineering principles, not for the purpose of making
1186 competing services perform less well but to make them perform
1187 more well.

1188 In one of the reasons that Comcast implemented the
1189 system that they got in so much trouble for a couple of years
1190 ago was because they had customer complaints that Vonage was
1191 not working well on their network. And they analyzed the
1192 traffic on their network to troubleshoot this problem that
1193 customers were reporting with Vonage's voiceover IP service
1194 and what they found was the rise of peer-to-peer traffic was
1195 causing delays for Vonage. And this is because peer-to-peer

1196 traffic puts enormous volume on the uplink side of a network
1197 that was engineered primarily to supply data in the downlink
1198 direction. And the reason it is engineered that way is
1199 because that simply is the way that data flows on the
1200 worldwide web and when you click on a website you send a
1201 small message upstream and what you receive downstream is,
1202 you know, 30, 50, 100,000 bytes.

1203 So the networks are engineered to behave asymmetrically.
1204 A new application comes along that actually puts more data on
1205 the uplink side then it draws down on the downlink side and
1206 it destabilizes the network engineering throughout the entire
1207 network. And so the engineering tools are applied to
1208 identify that problem and they made a crude attempt and they
1209 admit--I mean I am actually more positive about their
1210 attempts than they are. They admitted that their attempt to
1211 resolve that problem was done incorrectly and so the way that
1212 that should be done is in a more anonymous and more protocol-
1213 neutral manner where they simply collect data about the
1214 volume of traffic that individual users are putting on the
1215 network over a 15 minute period of time. So this is a
1216 beneficial use.

1217 In my written testimony, there is a little footnote
1218 where I try explain why I think the issue of deep packet
1219 inspection is so--there is so much animosity against it.

1220 Now, I think what is actually behind that is a dispute over
1221 two competing regulatory models for advanced
1222 telecommunication services like Internet and broadband. The
1223 traditional method has been described by FCC Commissioner
1224 McDowell as technology silos, where we regulate telecom one
1225 way. We regulate information services another way and every
1226 new technology that comes along becomes the subject of a new
1227 raft of regulations. Well, it turns out that technology
1228 silos approach with Title One, Title Two regulations isn't
1229 effective when you have competing services like voice and
1230 video that can be delivered across different platforms. And
1231 so there are a couple of different ways to address that
1232 problem and one solution that has been proposed is to go to a
1233 functional layering model where the different layers of the
1234 network are regulated according to different standards.

1235 So we treat carriers one way because that they are
1236 basically moving packets across a network. We treat web
1237 services providers a different way because they are on top of
1238 that infrastructure. But I think that approach which
1239 essentially is just rotating the silos model 90 degrees to
1240 the right exhibits a lot of the same problems because what
1241 you have is the ambiguity of services. E-mail is a service
1242 that can be provided by an ISP and traditionally is but it
1243 can also be provided by a web company like Google or Yahoo.

1244 Is there some reason why Google and Yahoo's e-mail should be
1245 regulated differently from an ISP's e-mail? I don't think
1246 there is. E-mail is e-mail is e-mail. It is a service.

1247 Mr. {Boucher.} Mr. Bennett, you are now about 2-1/2
1248 minutes over your time if you would wrap up.

1249 Mr. {Bennett.} I am sorry. I got too inspired.

1250 Mr. {Boucher.} That is quite all right.

1251 Mr. {Bennett.} So that is my pitch is that I think that
1252 rather than focusing on the technology, it makes more sense
1253 to look at the services themselves and to begin with the
1254 standards of proper disclosure and truth in advertising that
1255 any service should have.

1256 [The prepared statement of Mr. Bennett follows:]

1257 ***** INSERT 7 *****

|
1258 Mr. {Boucher.} Thank you very much, Mr. Bennett and
1259 thanks to each of our witnesses this morning for your
1260 informative testimony.

1261 So a question that I have all of you are invited to
1262 comment on this relates to whether or not we have anyone at
1263 the present time using network technologies for behavioral
1264 advertising purposes. NebuAd has gone. Is anyone using
1265 packet inspections specifically today for the kinds of
1266 activities that NebuAd I suppose is the way you pronounce
1267 this but NebuAd was using at the time this subcommittee had a
1268 hearing on that practice during the last Congress, Mr.
1269 Rotenberg?

1270 Mr. {Rotenberg.} Mr. Chairman, my understanding is that
1271 there is no provider in the United States right now that is
1272 using DPI for targeting in large measure because of the work
1273 that was done by this committee last year. But the activity
1274 is continuing in the United Kingdom and that is very
1275 interesting to watch both by the response of the companies,
1276 some of which have said that they will not participate, and
1277 also by the response of the European commissioners
1278 responsible for privacy protection who have said they are
1279 going to try to crack down on this practice. But my
1280 understanding in the U.S. is that it is not currently taking

1281 place.

1282 Mr. {Boucher.} Thank you. Do any of you have
1283 suggestions for other kinds of network technologies apart
1284 from the ones we focused on today and that would be
1285 specifically deep packet inspection, the new possible uses of
1286 cable set-top boxes and the GPS tracking chips that are now
1287 placed in some mobile devices? Those are the three we
1288 focused on today. Are you aware of any other similar kinds
1289 of technologies that carry significant privacy implications
1290 that we should keep an eye on, Ms. Harris?

1291 Ms. {Harris.} Mr. Chairman, I just think it is
1292 important to clarify and maybe this is Brian's to clarify and
1293 not me that GPS is not the only way that location is being
1294 collected for services. So I think there is somewhat of a
1295 misunderstanding that GPS chips and I would rather Brian
1296 describe it then I but, you know, I wouldn't want--I would
1297 rather we focus on location services because if you say GPS
1298 then it actually will not reach a lot of the mobile services
1299 that are going.

1300 Mr. {Boucher.} That is appropriate. Any further
1301 comment on that question, Mr. Rotenberg?

1302 Mr. {Rotenberg.} Well, this follows from Leslie Harris'
1303 point. If your concern, for example, is about mobile
1304 tracking in the network environment then I think you should

1305 also look at the issue of IP addressing. In other words, the
1306 designation that is associated with a device in the network
1307 can reveal a great deal of information about the user of the
1308 device and the location of the device. It is actually what
1309 enables services like Loopt, for example, to track users.

1310 Mr. {Boucher.} All right. Any further comment, Mr.
1311 Knapp?

1312 Mr. {Knapp.} Yeah, I mean I actually am not entirely
1313 sure about the IP address association but there are a wide
1314 variety of location technologies that enable these kind of
1315 applications consumers are enjoying. And, you know, I would
1316 just say that also speaks to why any consideration on
1317 legislation in this regard needs to be very considered so it
1318 is not sort of immediately put out of date by a new
1319 technology and broadly consider location information as you
1320 do other data.

1321 Mr. {Boucher.} Thank you, Mr. Knapp. Ms. Attwood?

1322 Ms. {Attwood.} Mr. Chairman, I would like to answer the
1323 question that I would have liked you to ask me and broaden I
1324 think your intent. I think it is important to understand
1325 that the device isn't the concern that should be the focus of
1326 a privacy hearing because technology will improve and
1327 advance. I think in the USA Today story about how there is
1328 concerns about using social networks by individuals in the

1329 security context, you know, there will be advances in
1330 technology and devices. I think the question is starting
1331 from the proposition of are there things that we need to be
1332 looking at as an industry relative to protecting privacy
1333 interests and in that regard I would agree.

1334 Mr. {Boucher.} Let me get to that in a subsequent
1335 question. I was just focusing for the moment on the presence
1336 of emerging technology. I wanted to make sure we were
1337 covering the waterfront in the terms of the technologies that
1338 we need to keep an eye on so but thank you for that. I am
1339 actually going to come to that now and I want to begin by
1340 commending both you and also Mr. McSlarrow on your announced
1341 intention to protect consumer privacy in association with the
1342 use of technologies that can reveal an extensive amount of
1343 information about those consumers. My precise question to
1344 you, to both of you, is whether you have developed privacy
1345 policies to the level of detail of the application of
1346 consumer opt-in as compared to consumer opt-out. Have you
1347 gotten to that level of detail in terms of formulating and
1348 announcing your consumer protection policies?

1349 Ms. {Attwood.} Well, with respect to the specific topic
1350 of DPI, we have in fact announced that we will not use DPI.
1351 We don't use it today and we will not use DPI in connection
1352 with behavioral advertising without the customer's express

1353 meaningful consent.

1354 Mr. {Boucher.} And does express meaningful consent
1355 imply opt-in?

1356 Ms. {Attwood.} It absolutely can imply opt-in. I am
1357 going to push all of you in the committee as we learn more
1358 about these issues to advance our thinking and our discussion
1359 about what we mean by opt-in. Opt-in is an old terminology.
1360 Opt-out is an old terminology.

1361 Mr. {Boucher.} In our thinking, it basically means that
1362 your customer would have to take an affirmative step of some
1363 kind in order to expressly authorize you to engage in the
1364 identification and tracking process. So checking a box,
1365 clicking a box on the website would be an example of opt-in.

1366 Ms. {Attwood.} It would absolutely be an example of a
1367 customer engagement and what we have committed to is that we
1368 will in fact bring the customer into that decision about how
1369 their information is used before we use any DPI for
1370 behavioral advertising. And I think really I commend and I
1371 encourage you to look at Loopt's way in which they have
1372 approached it and they have absolutely worked on a very small
1373 form which is a mobile device and made sure that customers
1374 not only check a box but actually engage with the service
1375 provider, understand what they are purchasing and therefore
1376 get the benefit of it.

1377 Mr. {Boucher.} So it is opt-in plus?

1378 Ms. {Attwood.} I would say it is engagement and it is
1379 in fact a complete transparency and customer control, yes.

1380 Mr. {Boucher.} Okay. Thank you. Mr. McSlarrow.

1381 Mr. {McSlarrow.} Mr. Chairman, as an industry I don't
1382 think we have made any announcement but I can, as you
1383 suggested, report that at least for the ISPs, when you are
1384 talking about user data providing the bedrock for behavioral
1385 targeted advertising, they recognize the burden has got to be
1386 a lot heavier. It has got to approximate and I sort of
1387 associate myself with Dorothy's comment about whether it is
1388 opt-in or not but the point is that the step, affirmative
1389 step taken by the consumer after engagement and education we
1390 have recognized is the necessary precondition to moving
1391 forward.

1392 Mr. {Boucher.} Okay. Thank you. Mr. Knapp, you as Ms.
1393 Attwood has suggested, are using a form of opt-in in order to
1394 gain your customers' consent before you engage in location
1395 activities using mobile devices. What brought you to that
1396 model? What were the considerations and can you describe how
1397 that works in your application?

1398 Mr. {Knapp.} Sure and I think the illustrations in the
1399 back of my testimony are great if members would like to turn
1400 to that and sort of see the flow that the user goes through

1401 but the key is and it is with all of these applications the
1402 users are choosing to access them and so, you know, in the
1403 case of Loopt they are choosing to download it from the AT&T
1404 deck or the Apple's iPhone, the App-store. They download it
1405 and then they need to sort of set-up Loopt to work for them.
1406 And it was very clear to us that users want to be in complete
1407 control of whether a company like Loopt was accessing their
1408 location information and then allowing them to share it with
1409 others. And so it was pretty key for us given that they were
1410 going to use our application to share it with others to make
1411 sure that they initially walk through a step to set it up
1412 that educated them about the application and the service.
1413 So, you know, I mean a lot of these key privacy principles go
1414 back even a few decades to 1980 when the OECD published those
1415 and I think, you know, in subsequent privacy practices. And
1416 that is also why I mentioned before with regard to location
1417 information it is certainly sensitive information but I think
1418 you can look at and as we did other privacy laws and
1419 principles that are out there and guidelines, and apply them
1420 broadly to information like location.

1421 Mr. {Boucher.} Thank you, Mr. Knapp. My time has
1422 expired. The gentleman from Florida, Mr. Stearns, is
1423 recognized for 5 minutes.

1424 Mr. {Stearns.} Thank you, Mr. Chairman. Mr. Rotenberg,

1425 I have had the opportunity to hear you as a panel witness
1426 particularly when I was chairman of the consumer trade and
1427 protection subcommittee. Although the bill is a little old,
1428 it was dropped in the 109th Congress, the Consumer Privacy
1429 Protection Act, HR1263, which my good friend, Mr. Boucher,
1430 was a co-sponsor. He and I worked together on this bill. Do
1431 you think that bill as it has been written could be used as a
1432 starting point for this? And how would you change it today
1433 for a general privacy bill for out of this subcommittee?

1434 Mr. {Rotenberg.} Thank you very much for the question,
1435 Mr. Stearns. I also want to commend you by the way because I
1436 do remember that series of hearings that you held on consumer
1437 privacy which I think were very important hearings. I would
1438 need to go back and look at the legislation that you and the
1439 Chairman had put together. I do recall thinking at the time
1440 that we needed to be sure that the policies gave consumers
1441 some meaningful control over their information. That it
1442 wouldn't be enough just for the consumers to be told the
1443 policy of the company and then to consent, opt-in or opt-out,
1444 but we really wanted to give consumers the assurance that for
1445 example security standards were being followed. One of the
1446 things that we have learned over the last few years of course
1447 is that we have problems today with security breaches in the
1448 U.S. and it impacts business and the Internet user. So I

1449 think that would be important. There is always this
1450 difficult issue of course of a State preemption. I
1451 appreciate that the businesses would like a national
1452 standard. That is a tough one.

1453 Mr. {Stearns.} That was one. If you might just take a
1454 moment and go back since you are an educator and you could
1455 give us a good sounding, it might be helpful for Mr. Boucher
1456 and I to have your written comments about the bill and what
1457 you think. Is anyone else on the panel familiar with the
1458 bill that I dropped, H.R. 1263, that Mr. Boucher and I who
1459 would like to comment on it? Yes, Ms. Harris.

1460 Ms. {Harris.} Mr. Stearns, I think we would have to go
1461 back and refresh our memory, as well.

1462 Mr. {Stearns.} Okay.

1463 Ms. {Harris.} You know, at the time I think we, you
1464 know, there were always as Marc has said, series of questions
1465 about preemption, about standard, just thinking about
1466 development since then, behavioral advertising we have to
1467 sort of put it in context but we would be glad to come back
1468 to you.

1469 Mr. {Stearns.} Okay. Mr. Bennett, you had mentioned in
1470 your opening statement about in some cases the difference
1471 between an ISP services and a web-based services, you know,
1472 if you are talking about sort of web-based services like

1473 Google and Microsoft and Yahoo, do you think they should be--
1474 have a separate type of privacy policy or is the privacy
1475 policy that we apply applicable to them too?

1476 Mr. {Bennett.} I think e-mail is e-mail and it doesn't
1477 matter whether it is provided by the ISP or by a web-based
1478 services provider. I think the exact same standards for
1479 disclosure and transparency should apply to a web-based
1480 service that is equivalent like e-mail is to services
1481 traditionally been provided by ISPs.

1482 Mr. {Stearns.} To your knowledge, are the people
1483 providing e-mail today, web-based services, are they scanning
1484 our e-mails for certain words? To your knowledge, could that
1485 be?

1486 Mr. {Bennett.} Google absolutely does. I mean the web-
1487 based e-mail services are primarily advertising supported
1488 because unlike the ISPs they don't collect a subscription
1489 fee. So some of them have an option where you can get the
1490 advertising taken off your e-mail.

1491 Mr. {Stearns.} But does that prevent the web-based
1492 service from still scanning if you click that?

1493 Mr. {Bennett.} I believe it would. I can't say that
1494 for a certainty.

1495 Mr. {Stearns.} But you are saying right now that most
1496 of these web-based services are scanning our e-mail for

1497 certain words using that as a double back to give us
1498 advertising so that when I go on one of these which I do, I
1499 see all these ads and sometimes these ads are for things that
1500 appear to me that I have just been interested in not too long
1501 ago.

1502 Mr. {Bennett.} Um-hum.

1503 Mr. {Stearns.} So if that is true, do you think that is
1504 considered something that should be part of a privacy bill so
1505 that consumers are aware when they go on their e-mail that
1506 their words are scanned, that their e-mail is being scanned?

1507 Mr. {Bennett.} I think it depends on a judgment that
1508 you have to make about consumer awareness. I mean it seems
1509 to me that people that subscribe to an e-mail service like
1510 Yahoo or Gmail are aware of the fact that it is an
1511 advertising supported service and I think Google does a
1512 pretty good job of disclosing the fact that they scan the e-
1513 mails for contextual clues so that they can put more relevant
1514 ads, you know, alongside the e-mails.

1515 Mr. {Stearns.} Yeah, Mr. McSparrow, the Chairman had
1516 mentioned the Project Canoe and it is being used I think to
1517 track consumers watching. I think you might just give us an
1518 idea what the status is of the cable industry with this
1519 Project Canoe, what it is really about and how it is being
1520 tracked and what the future is for the cable industry?

1521 Mr. {McSlarrow.} Sure, it is now called Canoe Ventures.

1522 It is a consortium of six cable operators.

1523 Mr. {Stearns.} Can you tell us who they are?

1524 Mr. {McSlarrow.} I should be able to remember that,

1525 Comcast, Time Warner, Bighthouse, Cablevision. I will have

1526 to get you the complete list.

1527 Mr. {Stearns.} Cox?

1528 Mr. {McSlarrow.} I believe Cox, yes.

1529 Mr. {Stearns.} Yeah, okay.

1530 Mr. {McSlarrow.} And I know I am missing somebody.

1531 Basically the idea is to build a platform to work with

1532 program networks and advertisers to allow them to deliver

1533 more relevant advertising to the consumer. The classic

1534 example used by the CEO of Canoe Ventures is the ideal would

1535 be to make sure you could deliver a dog food commercial to a

1536 household that has dogs, in the here and now.

1537 Mr. {Stearns.} So this is an interactive operation

1538 where there must be a remote for the customer on Comcast, for

1539 example, and when this program comes up they can hit a remote

1540 which will tell them yes they want it then that is a

1541 feedback, has information that the cable operator gives to

1542 the advertiser which in turn he puts an ad back in to give.

1543 Mr. {McSlarrow.} It could be.

1544 Mr. {Stearns.} Could be.

1545 Mr. {McSllarrow.} Today they only have two products that
1546 they are planning on launching and one uses just third-party
1547 demographics data. It doesn't have any set-top box user data
1548 at all.

1549 Mr. {Stearns.} No interaction.

1550 Mr. {McSllarrow.} The second one would be what you just
1551 described which would be a commercial comes up and you have
1552 an opportunity to hit a button and say yes I would like to
1553 order a pizza. So it is that built-in, opt-in system. In
1554 preparing for this hearing, I actually asked them the
1555 question whether or not they had any plans to use set-top box
1556 generated data for purposes of advertising. It is not even
1557 on the product road map but they do recognize if and when
1558 down the road they get to a point in time where they would
1559 have to take a look at that, they would have to comply fully
1560 with the Cable Act which exists today and I think they are
1561 very conscious of the privacy implications of everything they
1562 do but as I said it is not even on the product roadmap.

1563 Mr. {Stearns.} All right. Thank you, Mr. Chairman.

1564 Mr. {Boucher.} Thank you, Mr. Stearns. The gentlelady
1565 from California, Ms. Eshoo, is recognized for 5 minutes.

1566 Ms. {Eshoo.} Thank you, Mr. Chairman, and thank you to
1567 each of the witnesses. This has been a really a valuable
1568 experience to listen to each of you coming at the subject

1569 matter for the subcommittee today. First, Ms. Attwood, I
1570 didn't when you talked about opt-in, does AT&T support opt-
1571 in?

1572 Ms. {Attwood.} AT&T for the use of DPI for behavioral
1573 targeting, yes, we have said we will not use DPI for
1574 behavioral.

1575 Ms. {Eshoo.} Because you used the word engagement, you
1576 said we support engagement.

1577 Ms. {Attwood.} Yeah, I think engagement.

1578 Ms. {Eshoo.} You want to talk about weddings, we want
1579 to talk about this.

1580 Ms. {Attwood.} Yes, sure, I think engagement is
1581 actually a better way to describe what we are talking about
1582 which is customer awareness but.

1583 Ms. {Eshoo.} So you do support opt-in?

1584 Ms. {Attwood.} Yes.

1585 Ms. {Eshoo.} Okay. Now, in the last three years AT&T,
1586 as you know, has paid more than \$21 million to resolve FCC
1587 claims that it misused a customer's personal information.
1588 What is your policy moving forward to get away from that
1589 record?

1590 Ms. {Attwood.} We are very proud of our record is
1591 supporting our customers' privacy. I think you are referring
1592 to UPN issues.

1593 Ms. {Eshoo.} Well, \$21 million in fines is a lot. I
1594 don't know who else in the industry has paid that much and
1595 but we don't want past to be prolog and so I am giving you
1596 the opportunity to tell the subcommittee where you move--how
1597 you move forward and what kind of policy AT&T would support
1598 beyond opt-in?

1599 Ms. {Attwood.} So part of the success story in any fine
1600 and any enforcement action is the fact that we have committed
1601 to improve our policies and in fact stand up and acknowledge
1602 the cooperation and work with the regulatory agency in order
1603 to ensure the protection of the customer information at issue
1604 there. So we absolutely pledge to continue to work on that.

1605 Ms. {Eshoo.} Good. Okay. Now, on I have a couple more
1606 questions. Has AT&T used AudioScience.com to place ads on
1607 the web?

1608 Ms. {Attwood.} Not to my knowledge if you are asking
1609 AudioScience with respect to DPI solutions, is that what you
1610 are asking?

1611 Ms. {Eshoo.} Well, it is my understanding that that is
1612 the case is it?

1613 Ms. {Attwood.} No.

1614 Ms. {Eshoo.} I mean do you--does, has AT&T used
1615 AudioScience?

1616 Ms. {Attwood.} We do not use a DPI solution to place

1617 ads on our web, no.

1618 Ms. {Eshoo.} Does AudioScience.com notify customers
1619 when data is collected or you don't deal with them at all?

1620 Ms. {Attwood.} I am not familiar with the dealings with
1621 AudioScience. I am happy to get back to you on with respect
1622 to that particular vendor.

1623 Ms. {Eshoo.} Okay. I would appreciate that. To, Mr.
1624 McSlarrow and Ms. Harris, in Mr. Bennett's written testimony
1625 he says ``I fear the only way to ensure robust protection for
1626 personal privacy in the long run is to replace the open
1627 access advertising supported business model with one in which
1628 we pay for content and services.'' I guess this modern day
1629 ``modest proposal'' is one solution. I think it would
1630 destroy a free and open Internet and that it would in turn
1631 fix all of the privacy concerns that we have discussed today.
1632 But I think the real issue here is what you think or if you
1633 think that consumer privacy and a free and open Internet are
1634 compatible?

1635 Mr. {Rotenberg.} Yes, well Congresswoman I understand
1636 where Mr. Bennett is coming from. I mean there is the
1637 concern right now that if we continue down the unregulated
1638 advertising model that is sustaining the Internet, there is
1639 no stopping point. And I even raise in my testimony the
1640 related concern that this won't only be about privacy. This

1641 will be about web publishers because the content on the
1642 websites will become less valuable to the advertising
1643 networks as they learn more about the users. They will
1644 effectively bypass the content which will actually weaken the
1645 publishing industry. So I don't even think it is just
1646 privacy that is at risk in the unregulated advertising model.
1647 I think it is web-based publishing that is at risk, as well.
1648 Now, while I am sympathetic to his view, I do think
1649 advertising is important and can help sustain a lot of the
1650 Internet as long as limitations are established. That is
1651 really the key here. If we can say yes we need advertising.
1652 We understand that and there is a benefit here by having
1653 Internet with advertising but we are going to draw some lines
1654 and you are not going to get to do these tremendous profiles
1655 of users that currently taking place. I think that is a
1656 sustainable model. In fact, that is the tradition in the
1657 publishing world. You know, publishing up until recently had
1658 done very well for the user, for the publisher and for the
1659 advertiser but we are going down a road right now which I am
1660 afraid will actually lead to collapse.

1661 Ms. {Eshoo.} Kyle, you want to say something?

1662 Mr. {McSlarrow.} Well, I think the short answer is I
1663 think they are compatible. I think, you know, one of the
1664 great--I mean we can all, at least some of us can remember,

1665 you know, the day that the Internet was sort of
1666 commercialized but that is the world we live in and I think
1667 the great thing about the Internet is it is proven that you
1668 can take what was an old broadcast advertising model with a
1669 lot of waste and refine it in a way that allowed the services
1670 we have today. To me, the next step by keeping privacy in
1671 mind is to make that advertising model potentially even more
1672 relevant and more useful to advertisers. I just think it
1673 lists the entire Internet so I think we have to recognize
1674 privacy is an important part of it but I do think for the
1675 future of the Internet that kind of targeted advertising is
1676 going to be essential.

1677 Ms. {Eshoo.} Ms. Harris.

1678 Ms. {Harris.} Well, I remain skeptical about the value
1679 of the behavioral advertising in the long run but, you know,
1680 it is here and I think the, you know, at the end of the day
1681 it is can we get a privacy regime in place that is going to
1682 put consumers back in charge and be able to make choices.

1683 Ms. {Eshoo.} I agree.

1684 Ms. {Harris.} I think that if we are chasing each
1685 business model, each technology, we are not going to be able
1686 to do this and we have to step back and ask what is it that
1687 we want to give consumers the right to do in terms of
1688 controlling what is reasonable and put that in place.

1689 Ms. {Eshoo.} And in going back to the exchange I
1690 believe that you had with the Chairman, you see that as best
1691 being carried out, implemented how?

1692 Ms. {Harris.} Well, I think we need a law that is a
1693 privacy framework.

1694 Ms. {Eshoo.} Yes.

1695 Ms. {Harris.} That is, you know, that we move that has
1696 to do with data collection wherever it is collected and right
1697 now strong sectoral laws. We have cable law that is fairly
1698 strong. We really on the Internet except for if you make a
1699 privacy promise and fail to keep it then you have a FTC
1700 violation, you don't have any rules. We have some sectors
1701 that engage in self-regulation that is reasonably robust but
1702 that is not ultimately going to be an answer given how this
1703 is going.

1704 Ms. {Eshoo.} Because it is not tameless.

1705 Ms. {Harris.} It is not going to be enough.

1706 Ms. {Eshoo.} Thank you very much.

1707 Ms. {Harris.} Sure.

1708 Ms. {Eshoo.} Thank you, Mr. Chairman.

1709 Ms. {Boucher.} Thank you very much. Thank you, Ms.
1710 Eshoo. The gentleman from Florida is recognized for a
1711 unanimous consent request.

1712 Mr. {Stearns.} Thank you, Mr. Chairman. I just want to

1713 put the testimony of Scott Cleland, the president for
1714 Precursor, LLC. He testified before the Energy and
1715 subcommittee, our subcommittee on July 17, 2008, and I think
1716 it would be relevant to have his part of this hearing. So if
1717 you ask unanimous consent to be made a part thereof.

1718 Mr. {Boucher.} Without objection.

1719 [The prepared statement of Mr. Cleland follows:]

1720 ***** INSERT 9 *****

|
1721 Mr. {Boucher.} The gentlelady from Colorado, Ms.
1722 DeGette, is recognized for 5 minutes. I am sorry, 7 minutes
1723 in total.

1724 Ms. {DeGette.} Thank you very much. Thank you very
1725 much, Mr. Chairman. I want to follow-up on the line of
1726 questioning that Ms. Eshoo was talking about because I am
1727 concerned on the one hand I think DPI has shown to be an
1728 effective and an efficient way to deal with spam and other
1729 security issues. On the other hand, I am thinking here about
1730 consumer protection and the choices that people have to make
1731 in accessing services or Internet content. And listening to
1732 the witnesses talk about opt-in or consumer knowledge or
1733 whatever terminology you want to use about it, it really
1734 underscores for me something Ms. Attwood said which is we
1735 don't really know what we mean when we say consumer knowledge
1736 or assent. For example, with Mr. Knapp's company, we were
1737 impressed by all the levels of informed consent that you ask
1738 for but I also have, I am sure your company doesn't do
1739 behavioral advertising. That is not what you are getting the
1740 informed consent for, correct?

1741 Mr. {Knapp.} We will support our service with
1742 advertising.

1743 Ms. {DeGette.} Are you going to do behavioral

1744 advertising with DPI?

1745 Mr. {Knapp.} Generally no, DPI is not something that
1746 we--we are a mobile application.

1747 Ms. {DeGette.} Right, it is a different application.

1748 Mr. {Knapp.} Exactly.

1749 Ms. {DeGette.} So are you going to say to your
1750 consumers now we are going to monitor what we are going to
1751 use this technology to do behavioral advertising that is
1752 tailored toward you and your habits? Do you want to opt-in
1753 to that? Are you going to do that?

1754 Mr. {Knapp.} And we in fact we do. We are going to
1755 support Loopt through advertising.

1756 Ms. {DeGette.} No, that is not my question.

1757 Mr. {Knapp.} Sure.

1758 Ms. {DeGette.} Is that going to be part of the informed
1759 consent that you give?

1760 Mr. {Knapp.} Yes.

1761 Ms. {DeGette.} Okay. Good. Now, that is admirable
1762 because my question is to Mr. McSlarrow is that going to
1763 happen with all of the members of your association that that
1764 is the kind of informed consent that the consumers are going
1765 to have?

1766 Mr. {McSlarrow.} I think actually I need to back up. I
1767 represent not just ISPs but also networks and I make a

1768 distinction among them because and this is one of the points,
1769 there are many actors on the Internet. For the ISPs, yes, we
1770 recognize that there is a heavier burden to use the
1771 personally identified.

1772 Ms. {DeGette.} So they are going to say to people, I
1773 mean they are going to say to people now if you give informed
1774 consent what that means is that your communications are going
1775 to be tracked and tailored for behavioral advertising?

1776 Mr. {McSlarrow.} Yeah, I think the notice in disclosure
1777 has to be as robust as possible. I mean this has to be
1778 legible and the English people need to understand this is
1779 exactly what we are talking about.

1780 Ms. {DeGette.} That is great. Ms. Harris, you are
1781 nodding your head.

1782 Ms. {Harris.} We testified in front of this
1783 subcommittee last year on behavioral advertising saying that
1784 is what it is required. Frankly, we think it is required
1785 already under the Electronic Communications Privacy laws.
1786 Obviously, we want that incorporated into a Consumer Privacy
1787 law but that is the right answer. I think it is hard. I
1788 think given the fact that ISPs are in a position where they
1789 are not in daily contact with their users, you haven't made a
1790 decision to go to a site, the online environment has not done
1791 a good job yet with opt-out so I think this is a difficult

1792 step. It is a big commitment and it will be difficult to
1793 implement but it is the right choice.

1794 Ms. {DeGette.} Right. Well, I agree with that and I am
1795 happy to hear both of you say that you are going to do that.
1796 Ms. Attwood, is that also the intention of AT&T?

1797 Ms. {Attwood.} Yes and we stated that on several
1798 occasions with respect to our ISP service, yes.

1799 Ms. {DeGette.} That it would be because I think
1800 consumers now understand. I know when I sign up for some
1801 kind of Internet communication or whatever it says, you know,
1802 our policy is we do not sell or otherwise communicate your
1803 data to other people unless you check here so people get
1804 that. I am not sure they understand DPI or what that means
1805 and I am wondering, Mr. Rotenberg, is eager to address this
1806 issue.

1807 Mr. {Rotenberg.} Well, Congresswoman, I would like to
1808 join this chorus and certainly opt-in would be preferable to
1809 opt-out but I don't think it is sufficient. And I don't
1810 think it is sufficient because it won't be meaningful unless
1811 consumers actually understand what data about them is being
1812 collected and how it is being used.

1813 Ms. {DeGette.} That is my point.

1814 Mr. {Rotenberg.} And I think the mistake that is often
1815 made is that we place so much emphasis on a policy and so

1816 much emphasis on obtaining consent that the person who is
1817 actually being asked to make the decision really doesn't have
1818 any information to make the decision. So for many of these
1819 Internet-based techniques, people really need to know what
1820 information about them is being collected. Show it to me and
1821 who are you giving it to and for what purpose? Now, if the
1822 person is okay with all of that, then you say yes, that is
1823 consent.

1824 Ms. {DeGette.} That is exactly what I am trying to say.

1825 Mr. {Rotenberg.} Okay. Well, that is great.

1826 Ms. {DeGette.} And the reason why I am concerned about
1827 that is because I don't think that certainly people above a
1828 certain age like me, may not understand exactly how this data
1829 can be used or where it can go. People under a certain age
1830 don't have--I think of my two teenaged daughters. They may
1831 not have the sophistication to understand why that could be a
1832 problem which is why I think you have to have adequate
1833 disclosure and education.

1834 Mr. {Rotenberg.} Right and if I could say one more
1835 point because, you know, my children are on Facebook now and
1836 we spend a lot of time looking at privacy issues with
1837 Facebook. And one of the things that struck me is that young
1838 people are actually pretty sophisticated about what
1839 information they put up, what information they don't put up.

1840 And when the change of the terms of service changed for
1841 Facebook, they organized and objected and Facebook listened
1842 and there has been a very important process going on because
1843 the users of the service knew what was happening. But and
1844 here is a very important related point, the information about
1845 Facebook users that flows to advertisers and application
1846 developers, people know very little about and it is those
1847 applications that they don't have any meaningful control
1848 over.

1849 Ms. {DeGette.} That is right and so that is why I think
1850 we really we can say informed consent or we can say consumer
1851 awareness or whatever but we need to make sure that they
1852 understand exactly where that information is going.

1853 Mr. {Rotenberg.} Yes.

1854 Ms. {DeGette.} And I think everybody up here is shaking
1855 their heads so I think, Mr. McSlarrow, do you agree with that
1856 concept?

1857 Mr. {McSlarrow.} I totally agree with it and not only
1858 is it the right thing to do, I think it is good business.

1859 Ms. {DeGette.} Great. Okay. Thank you. Thank you
1860 very much, Mr. Chairman.

1861 Mr. {Boucher.} Thank you, Ms. DeGette. The gentleman
1862 from Illinois, Mr. Rush, the chairman of the Subcommittee on
1863 Consumer Protection is recognized for 5 minutes.

1864 Mr. {Rush.} Thank you, Mr. Chairman. And, Mr.
1865 Chairman, I want to begin by really thanking you for your
1866 comments earlier in this hearing. I want you to know that I
1867 look forward to working very vigorously with you and on this
1868 particular issue and look forward to our joint hearing that
1869 we will be having in the near future. Mr. Chairman, I am
1870 going to start out with some questions that I would like for
1871 all of the panel if they would just even provide either a yes
1872 or no answer. And the question I am going to get right to
1873 what I believe for me is the heart of the matter, do you
1874 think that Congress should pass consumer privacy legislation
1875 with regard to all of the communications network?

1876 Mr. {Rotenberg.} How many votes do I get? Yes.

1877 Mr. {Rush.} Well, from Chicago we will see where we
1878 wind up at and then we will add something to it. Okay. All
1879 right. I am beginning with you.

1880 Ms. {Harris.} Yeah, absolutely we need to develop a
1881 baseline consumer privacy bill that is based on fair
1882 information practices across all technologies. And frankly
1883 we need a bill that covers all collection and goes beyond
1884 this, you know, the media environment. We have got sectoral
1885 laws right now that hit some sectors and not others so I mean
1886 we need to do both and it is not clear to me it should be
1887 done separately. We need a baseline consumer privacy bill

1888 that has to do with data collection and obviously there is a
1889 need to reconcile the fact that we have different or no
1890 standards in media but from a consumer protection point of
1891 view, I think it is probably broader than that.

1892 Mr. {Rush.} Okay. The fellow next to you.

1893 Mr. {McSlarrow.} Okay. Mr. Chairman, no but I would
1894 like to be at the table when do.

1895 Mr. {Rush.} Okay. All right.

1896 Mr. {Rotenberg.} Yes, Mr. Chairman.

1897 Mr. {Rush.} Yes, okay.

1898 Ms. {Attwood.} I guess I would have to say it depends
1899 and certainly I can echo the comments that everyone has made
1900 about a broad based look. I encourage the kinds of
1901 discussions that we are having today but it may be premature
1902 and that is quite frankly so that we can get better educated
1903 and as an industry so we have an opportunity. There is a lot
1904 of complex relationships that govern this environment and in
1905 order to get a complete answer we really need to have the
1906 industry supportive and so I would urge us as an industry and
1907 working with out fellows in the public interest world and
1908 civil society to come up with a robust plan. That does not
1909 mean that legislation is not something that ultimately is at
1910 the end of that road but certainly right now the first step
1911 is discussion.

1912 Mr. {Rush.} All right. Please, yes sir?

1913 Mr. {Scott.} Yes, I agree a baseline privacy law would
1914 be a reasonable next step.

1915 Mr. {Rush.} Yes, okay.

1916 Mr. {Knapp.} This is my first hearing. Is maybe an
1917 acceptable answer? I think as a cutting edge innovative
1918 company that really wants to offer a service that users love
1919 and they want for free I, you know, I think a high level
1920 privacy framework that sticks by tried and true principles
1921 would be beneficial. But I do have concerns when laws get
1922 too specific or focus on a snapshot in a moment of time as I
1923 think has been mentioned here today and may get outdated an
1924 problematic for some companies like us who are trying to
1925 innovate and offer services for free to comply. And so those
1926 would be my concerns about that approach.

1927 Mr. {Rush.} All right. Go ahead.

1928 Mr. {Bennett.} Mr. Rush, I think I could support a bill
1929 like that if the emphasis was on disclosure rather than on
1930 prohibitions of particular practices. And one feature that I
1931 would like to see in it is that once a consumer has opted
1932 into a data collection service, I think you should get a
1933 regular reminder or the opt-in shouldn't be perpetual. So
1934 when you opt-in to a service it works for a year then you
1935 have to get a notice and you have a choice of opting in again

1936 because I don't know how many websites I have given
1937 permission to, to collect information on me over the years
1938 that I have completely forgotten about.

1939 Mr. {Rush.} So your answer is yes?

1940 Mr. {Bennett.} I answered yes.

1941 Mr. {Rush.} Okay. All right. Thank you. Mr.
1942 Rotenberg, since we need another vote from you. Why don't
1943 you answer again? I am just kidding. All right. The next
1944 question that I have is and please the same sequences for all
1945 the panel is do you believe that consumers should have the
1946 same sort of control if and how their information is
1947 selected? Do you believe that they should control if and how
1948 this information is used? Please answer a yes or no.

1949 Ms. {Harris.} I think that the question of use is an
1950 important one and it seems to me that when you are
1951 authorizing a collection you ought to also be authorizing the
1952 purposes or you are authorizing that it can be used for
1953 multiple purposes. But I don't think, you know, simply
1954 saying you can have my data or not have my data answers the
1955 question. We use your data for marketing, opt-in, don't opt-
1956 in. We use your data for, you know, I mean I think there are
1957 some uses of data which are transactional that, you know, if
1958 you are ordering a product I think separately saying you can
1959 use my data to do what is necessary to process this

1960 transaction seems unnecessary but for uses that are not
1961 directly connected for the initial purpose of collection it
1962 is just a standard fair information practice then I think yes
1963 of course you have to authorize that.

1964 Mr. {Rush.} Sure. Next gentleman.

1965 Mr. {McSllarrow.} I think in our case The Cable Act
1966 actually is a good example which says that when you give
1967 authorization for personally identifiable information, it
1968 doesn't take into account the use of that data for just
1969 rendering the business services. But once you go beyond that
1970 I think you do have to identify what the purpose is you would
1971 use it for.

1972 Mr. {Rotenberg.} Mr. Chairman, I would say yes and I
1973 would probably add in some other things too like ensuring
1974 security of the data that is collected and some access to the
1975 information and some accountability. I think the basic
1976 elements of a privacy bill and in fact The Cable Act is a
1977 good model or at least the pre-Patriot Act version was a good
1978 model from 1984. That is a good starting point.

1979 Ms. {Attwood.} Yes, we support transparency and
1980 control.

1981 Mr. {Scott.} Absolutely and I think beyond that I agree
1982 that the consumer is not only entitled to know that their
1983 data is being used but three other things. One is

1984 intentionality, the other is behavior and the third is
1985 outcome. Why do you want my information? What are you going
1986 to do with it? And what does that mean to me as a consumer?

1987 Mr. {Rush.} Yes.

1988 Mr. {Knapp.} Yes we agree with the principles of
1989 transparency and control, as well.

1990 Mr. {Rush.} Okay.

1991 Mr. {Bennett.} That is a yes for me, too.

1992 Mr. {Rush.} Thank you, Mr. Chairman. I appreciate you,
1993 sir.

1994 Mr. {Boucher.} Thank you very much, Mr. Rush, and we
1995 look forward to coordinating closely with you as we develop
1996 the joint hearing between our two subcommittees and then
1997 thereafter as we develop privacy legislation which we will
1998 put forward in tandem.

1999 Mr. {Rush.} Nice of you to say, Mr. Chairman.

2000 Mr. {Boucher.} And thank you for your presentation.

2001 Mr. {Rush.} You are a great Chairman.

2002 Mr. {Boucher.} Thank you very much. The gentleman from
2003 New York, Mr. Weiner, is recognized for 5 minutes.

2004 Mr. {Weiner.} Mr. Chairman, I won't take the full 5
2005 minutes. It strikes me that some of the what gets hairy here
2006 is saying is defining what it is that you are checking the
2007 box to do. For example, is you say I want help in deciding

2008 what other products are out there that are being sold that I
2009 might be interested in. It is a pretty tough box to word. I
2010 mean it is a pretty tough disclosure to have any real meaning
2011 but I think by and large, consumers do like that. I mean I
2012 like it when you go to Amazon and it says we also have this
2013 for you. So I think one of the problems that we often face
2014 is that disclosure has tipping point that if you want it
2015 until the point that there is so much of it that it ceases to
2016 really disclose anything. And I think the part of the
2017 challenge that we have is trying to come up with terms of art
2018 that truly do encapsulate what we are trying to do. For
2019 example, you know, would you like to be told about other
2020 products you might be interested in. Theoretically, that can
2021 be just about anything. I mean it is concise and it is crisp
2022 and it probably is worded in a way that will entice people to
2023 check a box and I don't know how you have a second line that
2024 says but you are going to get a lot of stuff and a lot of
2025 companies that might be far removed from this shoe purchase
2026 might be getting information. And so I mean can you offer us
2027 any guidance on how to make this type of disclosure opt-in,
2028 opt-out truly useful to consumers without us all having to
2029 retain, you know, to go to lawyers.com to read what I am
2030 getting at Amazon.com. I don't know who would be best to
2031 tackle that? Whoever leans forward first.

2032 Mr. {Rotenberg.} Well, I mean, Congressman, it is an
2033 excellent point and it is one of the reasons I have suggest
2034 in my testimony not to place too much emphasis on opt-in or
2035 opt-out as the basis for privacy protection. Given a choice
2036 between opt-in and opt-out from the consumers' perspective,
2037 opt-in is preferable because it means more control but for
2038 many of the reasons you described, it won't be adequate for
2039 real privacy protection. For example, no one agrees to a
2040 security breach. In other words, you may check a box and
2041 give a company some information and some magnetic tape is
2042 going to fall off the back of the truck. You certainly
2043 didn't agree to that so there has to be a way I think within
2044 privacy law to get it to a broader range of issues for many
2045 of the reasons your described.

2046 Ms. {Harris.} I agree with that. I think that the
2047 Congress has been stymied in moving that forward on privacy
2048 because of the sole focus being about opt-in and opt-out, and
2049 not looking more broadly at how to resolve some of these, you
2050 know, other questions. And we don't know how to give notice
2051 well in a way that consumers understand. You know, I think
2052 one thing to look to is we just passed landmark new privacy
2053 protections in the healthcare context and it could have
2054 gotten equally tied-up around opt-in and opt-out and it
2055 focused far more broadly, you know, about where sharing was

2056 appropriate and not appropriate, security protections. So
2057 while those, while there are places where consent is
2058 required, it is not just about that. And I think that we do
2059 get hung up sometime and we don't wind up with a framework so
2060 we need a framework. And we would start with fair
2061 information practices because that is transparency. That is
2062 collecting data only to the extent you need it for the
2063 transaction. It is giving people choices about other uses
2064 and it is making the explanation about those other uses.

2065 Mr. {Weiner.} Right but before Ms. Attwood adds to
2066 this, even that is complicated, right?

2067 Ms. {Harris.} Right, I am not saying this is easy.

2068 Mr. {Weiner.} Right, I mean just about the transaction,
2069 well you bought the stereo. You should know about--do you
2070 mind if we share information with this speaker company and
2071 then you get information about that. I mean I agree it is
2072 that opt-in and opt-out is not the only way to do this and we
2073 are going to go far beyond that. But we have grown kind of
2074 culturally accustomed to the idea of having places that we
2075 kind of agree to what goes on. You know, when my credit card
2076 company says oh yeah, well we told you about that. I am
2077 like, really that was page nine six months ago on the thing
2078 we told you about it. We are covered. So you are right,
2079 opt-in, opt-out is not everything but the way we have grown

2080 literate with how these things happen as citizens, there is
2081 some expectation that we are going to have some control over
2082 that.

2083 Ms. {Harris.} Oh absolutely, I am not suggesting that
2084 we shouldn't.

2085 Mr. {Weiner.} Right.

2086 Ms. {Harris.} I am saying that even that is much harder
2087 and has not been done well online in most instances so, you
2088 know, passing this framework is the beginning but the
2089 assumption that we are going to get these practices right
2090 overnight, no, we are not.

2091 Mr. {Weiner.} Go ahead, Ms. Attwood.

2092 Ms. {Attwood.} I just I guess I offer some hope in the
2093 context of if you approach this as a legal exercise then
2094 consent is something that is a, you know, it is a difficult
2095 proposition to get right. But if you approach this as
2096 actually what really is exploding online and the idea that in
2097 fact you are trying to get personalization and you are trying
2098 to get information that is all about me and you are trying to
2099 get a page that identifies my likes and dislikes, I have
2100 confidence that that in fact this industry using new and
2101 developing tools will be able to actually communicate more
2102 effectively to the customer and allow that kind of
2103 customization and that personalization to be an advance. If

2104 we think about this as a design feature, privacy is a design
2105 feature in what I am offering then it is in my interest as a
2106 commercial entity to make it very clear that proposition.
2107 That is why you see the success of Loopt. On one level, his
2108 service is extremely complicated. On the other level, the
2109 customer gets it right away, understands the value of
2110 proposition and that communication is something that as an
2111 industry I think I am optimistic that we can work to grow
2112 that communication and make it work for consumers.

2113 Mr. {Weiner.} Thank you, Mr. Chairman.

2114 Mr. {Boucher.} Thank you very much, Mr. Weiner. The
2115 gentlelady from the Virgin Islands, Ms. Christensen, is
2116 recognized for 5 minutes.

2117 Ms. {Christensen.} Thank you, Mr. Chairman, and this is
2118 a very interesting hearing for me. Privacy is an issue that
2119 is of very much concern to minority communities like the one
2120 I represent and it comes up whenever we talk about HIT and
2121 other issues related. Ms. Attwood, when you were asking
2122 about opt-in and opt-out and you talked about engagement it
2123 seemed as though you used that word deliberately and wanted
2124 to elaborate on it and I wanted to be give you an opportunity
2125 to explain what you mean by engagement.

2126 Ms. {Attwood.} Sure, I actually think Mr. Rotenberg
2127 said it a lot better and but I think everybody on the panel

2128 has discussed it that when we talk about opt-in and opt-out,
2129 we really are limited in the concept of what we are trying to
2130 discuss when it comes to really ensuring that the customer is
2131 part of the decision about the use of the information and
2132 that is a broader concept. That is a concept that is
2133 engaging. That is a concept that is enticing. That is a
2134 concept of control. Opt-in, we have all been a part of opt-
2135 ins. I think the Congressman from New York described it
2136 where, you know, it is pages and pages and pages where the
2137 company is entirely protected and there is a checked box but
2138 it is not. The customer is not in fact really participating
2139 in that decision, you know, and so I am hopeful this industry
2140 can in fact rally around the idea of really bringing the
2141 customer into that decision and it can happen in a broader
2142 way.

2143 Ms. {Christensen.} I am kind of old fashioned and I am
2144 trying to remember when I see those kinds of boxes, I just
2145 want to skip them. Do people usually answer them and or do
2146 you have to opt-in or opt-out, just for my information, not
2147 as a swear. Do you have to answer it?

2148 Ms. {Attwood.} If it is designed that way, I mean they
2149 are designed differently but there are some that are forced
2150 screens or box where you can't get past it unless you do
2151 something so yes. There are others that in fact don't

2152 require that but most times it is a service obligation to
2153 check that box.

2154 Ms. {Christensen.} And in the cases where you just
2155 ignore it and try to move on and you can, that is assumed to
2156 be an opt-out?

2157 Ms. {Attwood.} It would be possibly an opt-out. It
2158 really again depends on the design of that. It may be that
2159 you don't get the service.

2160 Ms. {Christensen.} Did you want to say something, Ms.
2161 Harris?

2162 Ms. {Harris.} Yeah, I do want to agree with Ms. Attwood
2163 on the question of can industry doing this. I mean in
2164 discussing this with Mr. Weiner, it is very hard but when
2165 industry chooses to do this, when they choose to do it sort
2166 of at the beginning and do privacy by design rather than
2167 privacy by law, it can be accomplished. Loopt is an example.
2168 There are several examples in the online healthcare space
2169 where from the very beginning this has been built in, in a
2170 way that consumers can use. So I, you know, it is hard to
2171 say that we are in this environment of such technological
2172 innovation and we can't figure out how to use that
2173 technological innovation to make this simpler. I think we
2174 can. I think frankly a privacy framework will encourage that
2175 but I do think at the end of the day it is going to have to

2176 be, you know, a combination. The law by itself in the
2177 absence of companies stepping up and doing that and that is
2178 what is going to have to happen.

2179 Ms. {Christensen.} Okay. I thought Mr. Bennett's
2180 suggestion of having to go back periodically and opt-in was a
2181 good one. Does that happen now and if doesn't, would you all
2182 support periodically having to go back and review that
2183 question?

2184 Mr. {Rotenberg.} We have actually recommended that the
2185 right way to understand consent is that you should be able to
2186 opt-in when you choose to have your data used in a way and
2187 then opt-out at the point that you want to discontinue the
2188 use and I think Mr. Bennett's comment captures that but any
2189 time you choose to leave a service--this came up recently
2190 with Facebook, for example.

2191 Ms. {Christensen.} Yeah.

2192 Mr. {Rotenberg.} Facebook wanted to tell users well you
2193 leave the service. We will keep your data and the user said
2194 well that is not right. I mean if we leave the service we
2195 want you to delete the data.

2196 Ms. {Christensen.} Right.

2197 Mr. {Rotenberg.} And Facebook agreed and I think that
2198 is people's intuition and it is really fair, and when
2199 companies go against it then there is a problem.

2200 Ms. {Christensen.} Right.

2201 Ms. {Harris.} I think it is going to be a very
2202 important concept for the ISPs if they are to move into this
2203 space because for some people who are not also using an ISP's
2204 e-mail service, they may not be communicating with their ISP
2205 except at, you know, initially to sign up or get a bill so
2206 the potential to think about screens that come on, you know,
2207 that explain what you agreed to and give you a choice to
2208 change your mind, I think it is going to be a critical part
2209 of it.

2210 Mr. {Scott.} It strikes me that whether we are talking
2211 about reminders which I think is a great idea or engagement
2212 or clarity and transparency, we are really talking about our
2213 different forms of consumer education because the real
2214 problem is that most consumers don't have any idea what the
2215 10,000 words of six point font means when they check the box
2216 at the bottom and oftentimes, sometimes those boxes are pre-
2217 checked or you can't buy the shoes unless you check the box
2218 and so in many ways I think we need to be thinking about ways
2219 to help consumers understand exactly what it is that they are
2220 signing up for and what that means and what comes to my mind
2221 is the little glossy one-pager that my power company sends me
2222 every winter to try to advise me on how to save money on my
2223 power bills. It has got pictures. It is in big letters. I

2224 read it. I have actually found some helpful tips there.

2225 That is sort of is what I think of as engagement when I hear

2226 you say that and I think that is the kind of consumer

2227 education that can help us fix this problem.

2228 Ms. {Christensen.} Thank you. Thank you, Mr. Chairman.

2229 Mr. {Boucher.} Well, thank you very much, Ms.

2230 Christensen. I want to say thank you to all of the witnesses

2231 for their extremely informative testimony today. This has

2232 been an engaged conversation and as we close this hearing, I

2233 simply want to note that I personally concur completely with

2234 the suggestions that many have made here over the course of

2235 the last hour that what is needed is not just a decision

2236 between opt-in and opt-out but also a framework for privacy

2237 protection. And I hasten to note that the legislation that

2238 Mr. Stearns and I put forward some several years ago which

2239 will be the starting point and the foundation for our privacy

2240 bill this year, contains exactly the kinds of formulas that

2241 many on the panel have suggested and that is that any service

2242 that collects information about a customer must disclose what

2243 information that is collected and how that information is

2244 used and then provide the appropriate opportunity for that

2245 customer to act on the information, whether that be by opt-in

2246 or opt-out. So opt-in taken by itself, is meaningless.

2247 There has to be an adequate description of what conduct the

2248 particular user is authorizing for it to have content and
2249 meaning and offer real protection. We get that and that will
2250 be very clearly a part of the foundation of the measure that
2251 we move forward with later.

2252 So with that having been said and acknowledged, let me
2253 thank this panel for its contributions to our understanding
2254 of the network technologies that have privacy implications
2255 for users and suggest that we probably are going to
2256 consulting with you at greater length as we move forward to
2257 have out joint hearing with the other subcommittee and also
2258 to draft this legislation. You have been very helpful to us.
2259 We appreciate your participation and with that said, this
2260 subcommittee stands adjourned.

2261 [Whereupon, at 12:10 p.m., the subcommittee was
2262 adjourned.]